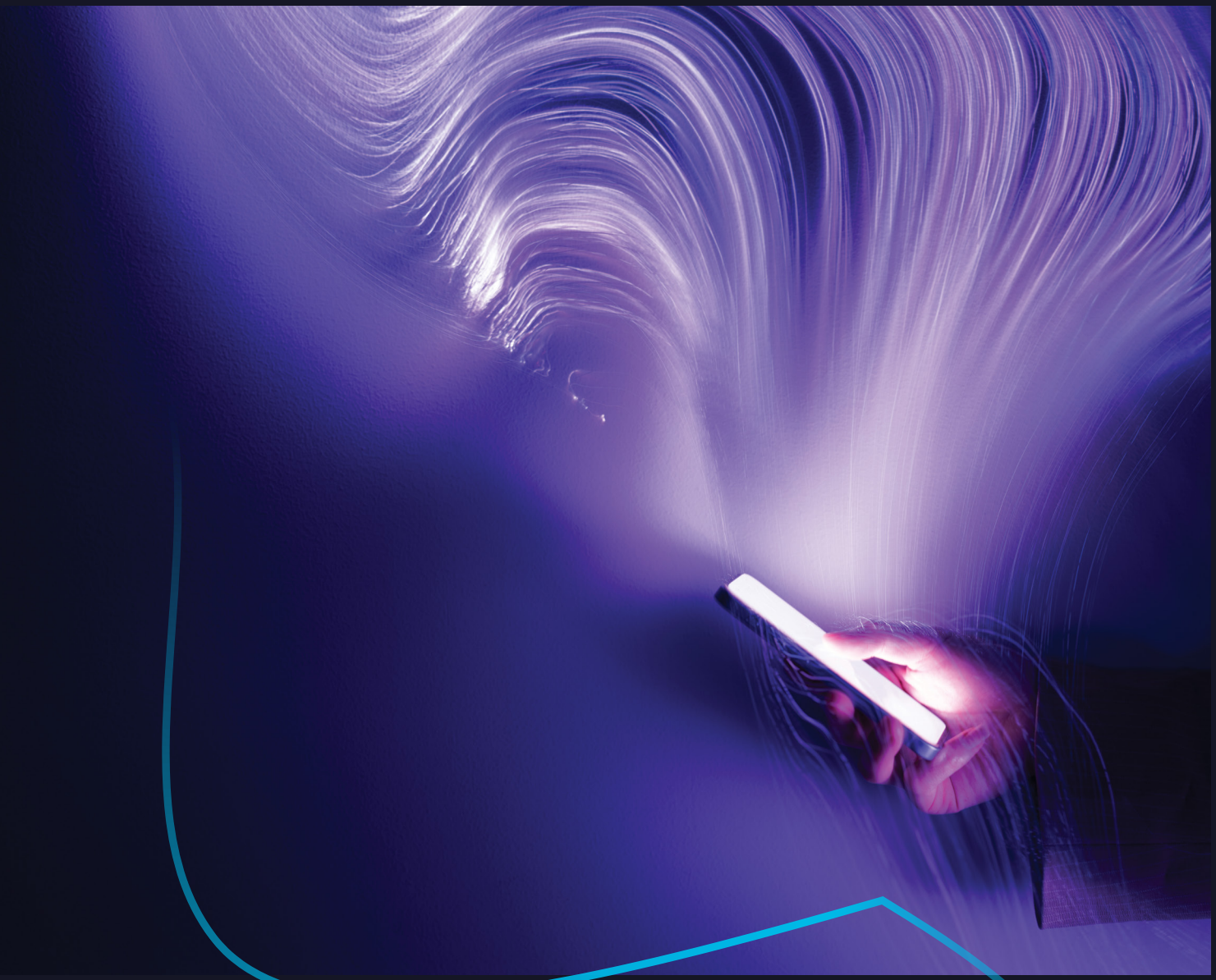


Außerhalb der EU – wenn die *DSGVO* nicht ausreicht

Deutsche Unternehmen und ihr Umgang mit Datenschutzgesetzen aus Drittstaaten

Capgemini invent

Vorwort

Die Datenschutz-Grundverordnung (DSGVO) ist eine von der Europäischen Union (EU) erlassene Verordnung, die am 25. Mai 2018 in Kraft getreten ist und den Datenschutz innerhalb der EU reguliert. Sie legt fest, wie mit personenbezogenen Daten umzugehen ist. Die DSGVO hat eine extraterritoriale Reichweite, sodass sie für alle Unternehmen und Organisationen gilt, die personenbezogene Daten von Personen innerhalb der EU erheben, verarbeiten oder speichern – unabhängig davon, ob eine EU-Ansässigkeit besteht. Die Verordnung soll europäischen Bürger*innen mehr Kontrolle über ihre personenbezogenen Daten geben und Unternehmen für den Umgang mit diesen Daten zur Verantwortung ziehen. Verstöße gegen diese Verordnung können erhebliche finanzielle und rechtliche Konsequenzen nach sich ziehen.

Seit dem Inkrafttreten der DSGVO haben weltweit immer mehr Länder außerhalb der EU eigene Datenschutzbestimmungen erlassen – in vielen Fällen ebenfalls mit extraterritorialer Wirkung. Folglich können sie auch für Unternehmen in Deutschland Anwendung finden, sofern diese personenbezogenen Daten in Drittstaaten verarbeiten oder die Daten von Bürger*innen dieser Staaten verarbeiten. Durch diesen weltweiten Trend müssen deutsche Unternehmen ihre Geschäftstätigkeit im EU-Ausland an die lokalen Datenschutzbestimmungen anpassen. Eine erhebliche Herausforderung besteht jedoch darin, dass in nahezu jedem Land unterschiedliche Datenschutzbestimmungen gelten. Daher ist spezifisches Wissen über die jeweiligen Regelungen erforderlich. Es ist von enormer Bedeutung, die lokalen DS-Bestimmungen zu verstehen und sich mit verschiedenen Verordnungen auseinanderzusetzen.

Vor diesem Hintergrund haben wir in der vorliegenden Studie das Verständnis und den aktuellen Stand der Umsetzung von Maßnahmen zu Nicht-DSGVO-Richtlinien durchgeführt. Die betrachteten Kernfragen sind:

1. Inwieweit haben deutsche Unternehmen ein Verständnis von internationalen Datenschutzvorschriften, insbesondere im Vergleich zur DSGVO?

2. Welche sind die wichtigsten Herausforderungen in Bezug auf Datenschutzvorschriften in Drittstaaten?

3. Wie können diese Herausforderungen gemeistert werden?

Zur Beantwortung dieser Fragen haben wir eine quantitative Umfrage unter deutschen Unternehmen durchgeführt, deren Ergebnisse in diesem Report dargestellt und analysiert werden. Zudem wurde eine nahezu identische Befragung in Österreich durchgeführt. Wichtige Erkenntnisse dieser Studie wurden in diesem Dokument mit den Ergebnissen aus Deutschland in Relation gesetzt, um einen besseren Überblick über das Verständnis der Datenschutzlandschaft in den beiden Ländern zu generieren. Außerdem befassen wir uns mit den wesentlichen Herausforderungen deutscher Unternehmen mit Blick auf die erfolgreiche Umsetzung von Datenschutzrichtlinien außerhalb der Europäischen Union. Abschließend werden verschiedene Maßnahmen vorgestellt, die einen optimalen Zugang zum Verständnis des internationalen Datenschutzes ermöglichen.

Inhalt

DSGVO als Trendsetter

Seit 2018 hat 68% der Weltbevölkerung ein neues oder aktualisiertes Datenschutzrecht erhalten

früher DSGVO
2018 2019 2020 2021 2022 2023

Kanada

Kanada verfügt über zwei Datenschutzgesetze, welche Unternehmen und öffentliche Institutionen regulieren. Darüber hinaus verfügen die Provinzen Alberta, British Columbia und Québec über regionale Gesetzgebung für den Privatsektor.

Europäische Union

Seit 2018 stärkt die DSGVO den Datenschutz und das Recht auf Privatsphäre in Europa.

Japan

Seit April 2022 werden personenbezogene Daten in Japan durch eine überarbeitete Fassung des nationalen Datenschutzgesetzes „APPI" reguliert. Zu den wesentlichen Veränderungen zählen dabei neue Anforderungen bei der Pseudonymisierung, Meldepflichten bei Datenpannen und erhöhte Strafen.

USA

Seit 2020 ist vor allem das kalifornische Datenschutzgesetz „CCPA" prägend für die Regulierung der Verarbeitung personenbezogener Daten in den USA. Mangels einer nationalen Gesetzgebung ist die Datenschutzlandschaft äußerst komplex und selbst in einzelnen Bundesstaaten finden sich regionale Spezifika.

China

Seit 2021 regeln insbesondere das „PIPL" und das „Data Security Law" in China den Schutz personenbezogener Daten. Die Missachtung chinesischer Datenschutzauflagen kann mit Strafen von bis zu EUR 6,4 Millionen oder 5% des Jahresumsatzes eines Unternehmens geahndet werden.

Mexiko

Strafen für Datenschutzverstöße können in Mexiko mit bis zu EUR 1,3 Millionen oder fünf Jahren Haft geahndet werden. Seit 2009 steht das Recht auf Privatsphäre sogar in Artikel 6 der mexikanischen Verfassung.

Indien

Nachdem der oberste Gerichtshof Indiens zu der Entscheidung gekommen ist, dass das Recht auf Privatsphäre ein Grundrecht darstellt, hat die Regulierung von Datenschutz wieder Fahrt aufgenommen.

Argentinien

Gemäß EU-Angemessenheitsbeschluss verfügen personenbezogene Daten in Argentinien über ein vergleichbares Schutzniveau wie in der EU. Jedoch gibt es unterschiedliche Anforderungen an die Datenverarbeitung. So haben Unternehmen nur 10 bzw. 5 Tage Zeit, um eine Datenauskunft oder eine Datenberichtigung durchzuführen.

Brasilien

Laut dem brasilianischen Datenschutzgesetz „LGPD" können bis zu EUR 8 Millionen bei Verstößen fällig werden. Trotz einer grundsätzlichen Nähe zur DSGVO gibt es beispielsweise Unterschiede bei der Rechtmäßigkeit von Verarbeitungstätigkeiten oder auch den Meldepflichten bei Datenpannen.

Südafrika

Seit Juli 2021 müssen Unternehmen mit dem südafrikanischen Datenschutzgesetz „POPIA" konform sein. Dazu gehört unter anderem auch die Pflicht der Registrierung eines sogenannten „Information Officers" bei der südafrikanischen Aufsichtsbehörde.

Australien

In Australien ist das Datenschutzregime durch nationale und regionale Gesetzgebung gekennzeichnet. Mit dem „CDR" steht vor allem die Regulierung personenbezogener Daten von Konsumenten im Fokus. Dabei wird das Gesetz seit 2020 gestaffelt nach Industrien eingeführt.

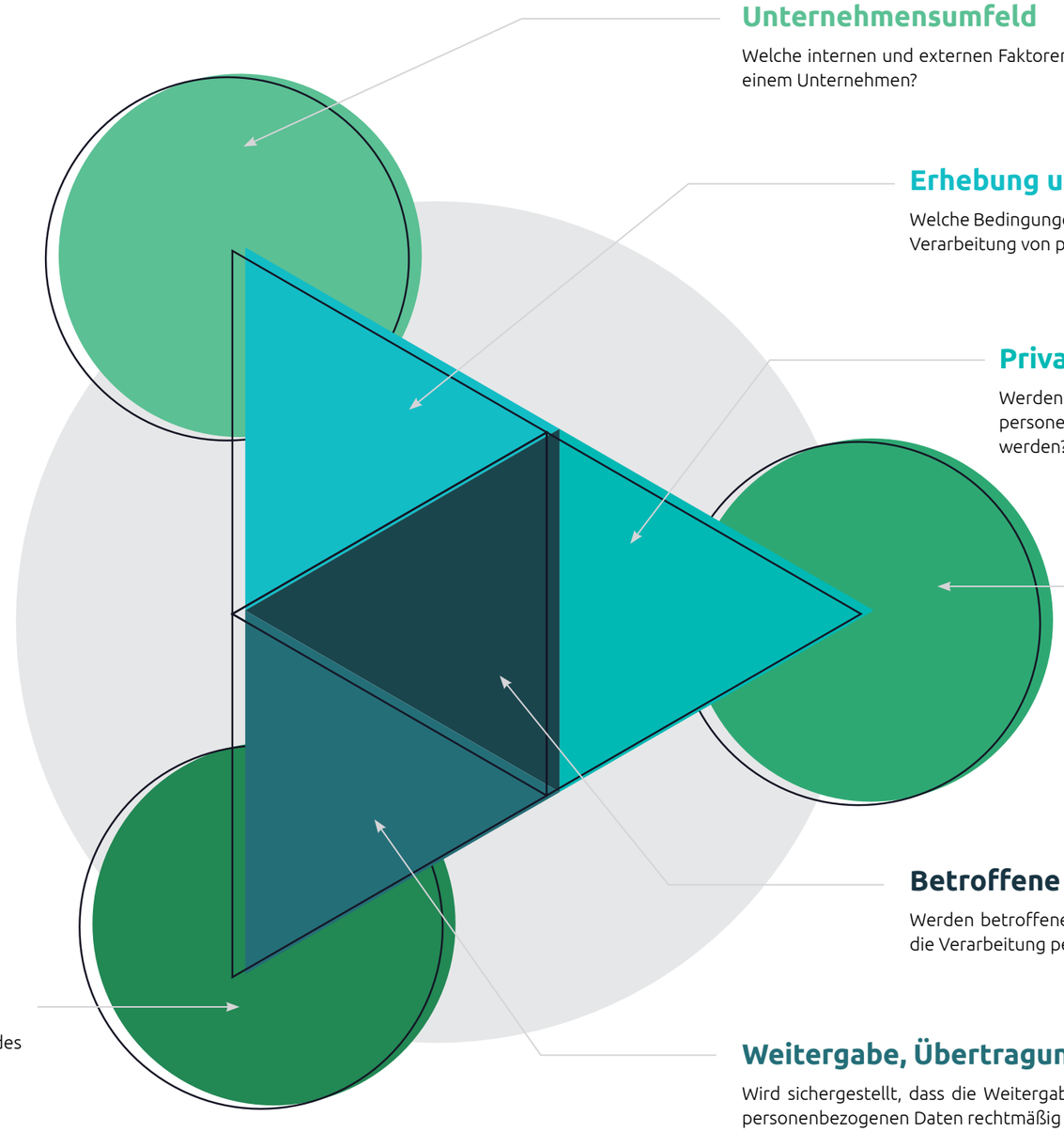
Nachhaltige Datenschutzorganisation

Datenschutz muss unternehmensweit gelebt werden

Wir durften bereits viele Unternehmen bei ihrer Transformation begleiten und konnten beobachten, wie die Einführung der DSGVO deutsche Unternehmen nachhaltig verändert hat. Der Stellenwert von Daten wurde unternehmensweit gestärkt. Unternehmen haben bereichsübergreifend die Tragweite der Verarbeitung von personenbezogenen Daten erkannt und verstanden, dass alle Mitarbeiter*innen dazu beitragen müssen diese zu schützen.

In unseren Projekten stellen wir immer wieder fest, dass im Sinne der Compliance zahlreiche Rollen, Verantwortlichkeiten und Prozesse geschaffen werden. Doch was nützt ein gutes Konzept, wenn die angestrebte Compliance nicht durch eine gelebte Datenschutzkultur nachhaltig etabliert wird? Wir sind der Meinung, dass Datenschutz eine kollektive Anstrengung eines gesamten Unternehmens darstellt und eine kontinuierliche Aufgabe aller Mitarbeiter*innen ist. Im Rahmen dieser Studie haben wir die Bausteine einer nachhaltigen Datenschutzorganisation genauer beleuchtet und uns die Frage gestellt, ob eine gute DSGVO-Compliance Unternehmen den Umgang mit internationalen Datenschutzanforderungen erleichtert.

Eine nachhaltige Datenschutzorganisation benötigt eine gelebte Datenschutzkultur und einen hohen Reifegrad etablierter Datenschutz-Compliance Maßnahmen. Entlang dieser beiden Dimensionen haben wir im Rahmen dieser Studie deutsche Unternehmen befragt.



Datenschutzkultur

Datenschutz-Compliance

Unternehmensumfeld

Welche internen und externen Faktoren beeinflussen Datenschutz in einem Unternehmen?

Erhebung und Verarbeitung

Welche Bedingungen werden für die rechtmäßige Erhebung und Verarbeitung von personenbezogen Daten erfüllt?

Privacy by Design/Default

Werden Prozesse und Systeme so gestaltet, dass personenbezogene Daten nur zweckbestimmt verarbeitet werden?

Stakeholder Management

Wie werden die Stakeholder innerhalb des Unternehmens eingebunden?

Betroffene Personen und Behörden

Werden betroffene Personen und Behörden angemessen über die Verarbeitung personenbezogener Daten informiert?

Weitergabe, Übertragung und Offenlegung

Wird sichergestellt, dass die Weitergabe, Übertragung und Offenlegung von personenbezogenen Daten rechtmäßig ist?

Leadership

Wie wird Datenschutz innerhalb des Unternehmens vorgelebt?

Mehr als die Hälfte der befragten Unternehmen hat ein Bewusstsein für die Bedeutung externer Faktoren aus Nicht-DSGVO-Ländern

Unternehmensumfeld

Unabhängig von Branche und Produktportfolio wirken externe wie interne Faktoren auf die Datenschutzorganisation eines Unternehmens ein. International tätige Unternehmen sehen sich durch den weltweiten Vertrieb ihrer Produkte und Services mit einer Vielzahl von Datenschutzanforderungen und deren extraterritorialen Anwendbarkeit konfrontiert. Externe Faktoren fallen in Abhängigkeit der Geschäftsmodelle und internationalen Ausrichtung deutscher Unternehmen unterschiedlich stark aus. Unternehmen, die in verhältnismäßig wenigen Nicht- DSGVO-Ländern aktiv sind und dadurch ihre Datenschutzorganisation nur sehr begrenzt auf lokal geltendes Datenschutzrecht angepasst haben, unterschätzen womöglich die Risiken einer Nicht-Compliance mit lokalen rechtlichen Anforderungen.

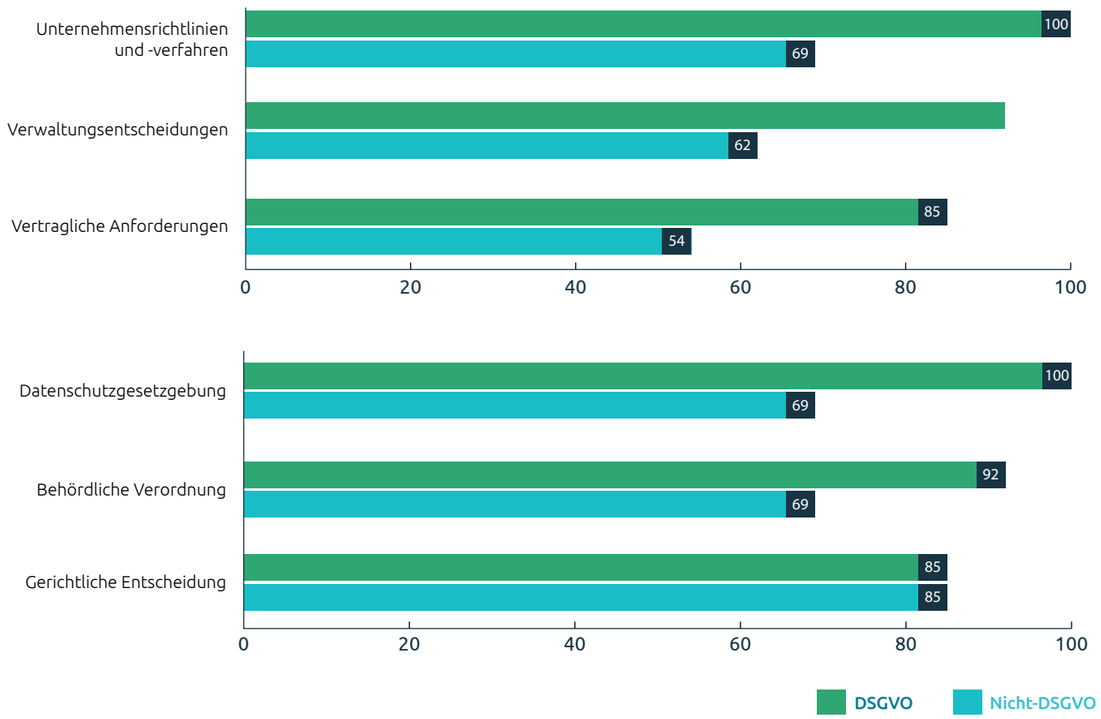
Neben den externen bestimmen auch interne Faktoren maßgeblich den Reifegrad der Datenschutzorganisation eines Unternehmens. Unabhängig von der internationalen Ausrichtung wirken sich unter anderem die individuellen Unternehmensrichtlinien und -verfahren auf den Umgang mit Datenschutzanforderungen aus.

In Bezug auf die internen Faktoren gaben sämtliche befragten Unternehmen an, dass sie die Unternehmensrichtlinien und -verfahren der DSGVO als entscheidende Elemente zur Erreichung ihrer Datenschutzziele berücksichtigt haben. Verwaltungsentscheidungen wie beispielsweise interne Entscheidungen der Rechtsabteilung sowie vertragliche Anforderungen, die von den geschäftlichen Gegebenheiten abhängen, wurden als weniger signifikant erachtet. Im Vergleich zu internen Faktoren haben externe Faktoren, insbesondere im Kontext der Nicht-DSGVO-Länder, einen leicht geringeren Stellenwert. Gemessen an der österreichischen Vergleichsstudie wird ihnen dennoch fast doppelt so große Relevanz zugeschrieben. So erachten fast zwei Drittel der deutschen Unternehmen gerichtliche Entscheidungen aus Nicht-DSGVO-Ländern (z.B. laufende/ vergangene Gerichtsverfahren) als einen relevanten Faktor, während dies nur für ein Drittel der österreichischen Unternehmen gilt.

Zusammenfassend sind sich deutsche Unternehmen der Bedeutung interner als auch externer Faktoren zwar bewusst, jedoch besteht im Nicht-DSGVO-Kontext noch Verbesserungsbedarf. Dennoch lässt sich festhalten, dass im nationalen Vergleich mit Österreich das Bewusstsein deutscher Unternehmen bereits deutlich stärker ausgeprägt ist.

Diagramm 1:

Wie viele der befragten Unternehmen erachten die genannten internen Faktoren, in Bezug auf ihr Unternehmensumfeld und deren Auswirkung auf ihre Datenschutzziele, als relevant oder sehr relevant?



Ein international tätiger Handelskonzern wurde 2022 in einem noch nicht rechtskräftigen Verfahren zu einem Bußgeld in Höhe von EUR 8 Millionen verurteilt, da Kunden über die Verarbeitungszwecke ihrer Daten nicht ausreichend informiert wurden.

Deutsche Unternehmen sind sich einig über die Relevanz externer Stakeholder in Bezug auf die Verarbeitung personenbezogener Daten

Stakeholder Management

Um Datenschutzvorgaben im Unternehmen gesetzeskonform umsetzen zu können, ist ein regelmäßiger Austausch mit internen und externen Stakeholdern notwendig. So sind Datenschutzbehörden im heimischen und internationalen Markt auf der Seite der externen Stakeholder von besonders hoher Bedeutung. Einerseits obliegt ihnen die operative Durchsetzung der Regulatorik, andererseits sind sie der Ansprechpartner, welcher dem regulierenden Gesetzestext am nächsten ist. So können sie bei der Umsetzung und Erfüllung von Auflagen unterstützen und datenschutzrechtliche Anforderungen spezifizieren. Neben diesen und weiteren externen Stakeholdern müssen auch die Ansprechpartner*innen im eigenen Unternehmen über Datenschutzmaßnahmen informiert und für notwendige Aktivitäten mobilisiert werden. Beispielsweise haben auf der Seite der internen Stakeholder die Prozessverantwortlichen des jeweiligen Unternehmens für die Umsetzung von Datenschutzrichtlinien eine Schlüsselrolle inne, da sie die Vorgaben in die Abläufe integrieren müssen.

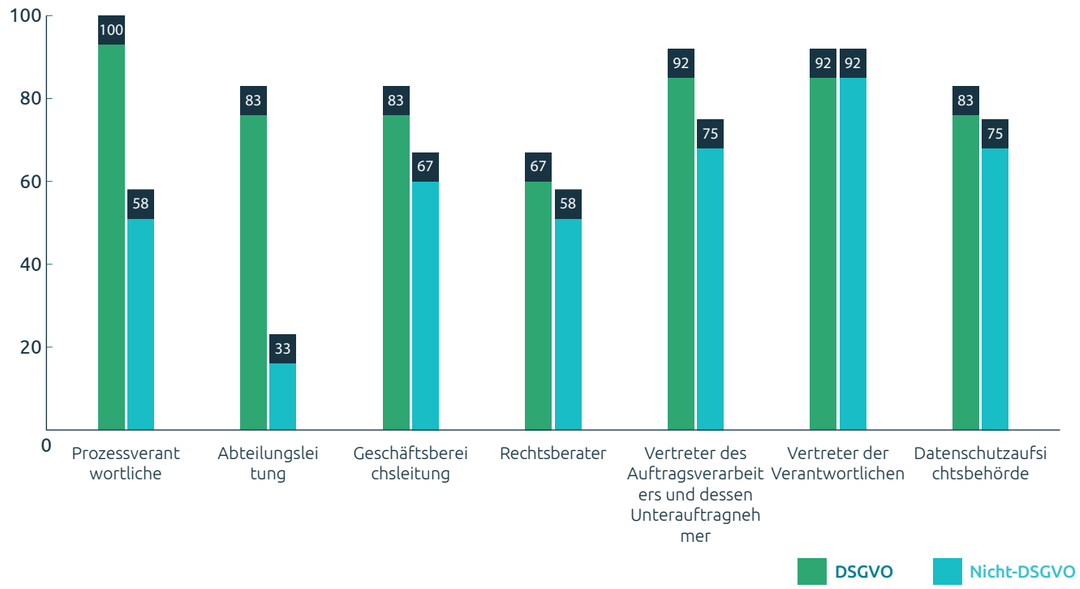
Wir haben untersucht, welche Relevanz die unterschiedlichen Stakeholder im Umgang mit personenbezogenen Daten aus Sicht deutscher Unternehmen haben. Bei der Verarbeitung personenbezogener Daten sollten die befragten deutschen Unternehmen eine unterschiedliche Relevanz für verschiedene interne und externe Stakeholdergruppen festlegen. Während hinsichtlich der Relevanz externer Stakeholder Einigkeit unter den deutschen Unternehmen besteht, zeigen sich bei den internen Stakeholdern deutliche Meinungsunterschiede. So sehen alle betrachteten Unternehmen die Prozessverantwortlichen als relevante Ansprechpartner für DSGVO-Themen. Im Nicht-DSGVO-Kontext sind es hingegen nur ungefähr die Hälfte der befragten Unternehmen.

Die Abteilungsleitung wird als relevant für DSGVO-Themen, jedoch als weniger relevant für Nicht-DSGVO-Themen erachtet. Lediglich bei der Relevanz der internen Geschäftsbereichsleitung unterscheiden sich die Meinungen nicht stark voneinander. So erachten zwei von drei Unternehmen die Geschäftsbereichsleitung als relevante*n Ansprechpartner*in für Nicht-DSGVO-Richtlinien. Dies ist besonders im Vergleich zur österreichischen Studie ein hoher Wert, da diese dort 43% der Fälle als relevante*r Ansprechpartner*in herangezogen wird.

Insgesamt werden die externen Stakeholder sowohl über DSGVO- als auch Nicht-DSGVO-Themen als relevantere Ansprechpartner*innen gesehen. Dieses Ergebnis ist gegensätzlich zur österreichischen Studie: Dort wird internen Stakeholdern eine höhere Relevanz zugeschrieben.

Diagramm 2:

Wie viele der befragten Unternehmen erachten nachfolgende externe und interne Stakeholder bei der Verarbeitung personenbezogener Daten für wichtig oder sehr wichtig?



Kennen Sie bereits die „Cyberspace Administration of China (CAC)“, die als der Super-Regulator des chinesischen Datenschutzrechts bezeichnet wird? Oder das chinesische „Ministerium für Industrie und Informationstechnik (MIIT)“, das Unternehmen aufgrund von Datenschutzverletzungen den Zugang zu IT-Systemen oder den Betrieb von Websites und Apps verbieten kann? Möglicherweise haben Sie aber auch schon vom „Ministerium für Öffentliche Sicherheit (MPS)“ gehört, dem unter anderem die chinesische Polizei untersteht? All diese Institutionen beeinflussen den Datenschutz in China und betreuen ein Geflecht diverser Datenschutz- und Informationssicherheitsgesetze.

Bei lediglich einem Drittel der befragten Unternehmen setzt die Top-Führungsebene Datenschutz-Reporting erfolgreich um

Leadership

Leadership und Unternehmenskultur stehen in einer starken Wechselwirkung. Während Leadership maßgeblich die Kultur einer Organisation gestaltet, hat die Unternehmenskultur einen Einfluss auf den Führungsstil und die damit verbundenen Werte und Schwerpunkte. Auch das Thema Datenschutz und die Antwort auf die Fragestellung, welchen Stellenwert dieser innerhalb der Organisation einnimmt, stehen in unmittelbarer Abhängigkeit dazu, ob Datenschutz als innovationshemmend und lästig oder als integraler Bestandteil des Geschäftsmodells gesehen und vom Leadership verstanden wird.

Eine ehrliche Antwort auf diese Frage zu finden, fällt vielen Unternehmen schwer. Daher haben wir gefragt, wie Führungskräfte deutscher Unternehmen Führungsstärke in Bezug auf den Schutz personenbezogener Daten zeigen können.

Innerhalb der Studie wurden sechs Maßnahmen bewertet, wie Führungskräfte in deutschen Unternehmen ihre Führungsstärke hinsichtlich des Schutzes personenbezogener Daten zeigen können. Der auffälligste Punkt hierbei ist, dass bei nur jedem dritten Unternehmen die Top-Managementebene

Führungsstärke in der Umsetzung eines regelmäßigen Datenschutz- Reportings aufzeigt. Dies gilt sowohl im Nicht-DSGVOKontext als auch im DSGVO-Kontext. Dadurch kann es den Führungskräften schwerer fallen, einen Überblick über aktuelle Datenschutzentwicklungen zu erhalten. Dazu passend gibt es nur bei der Hälfte der Unternehmen im Nicht-DSGVO-Kontext eine angemessene Kommunikation innerhalb der Organisation in Bezug auf den Schutz personenbezogener Daten.

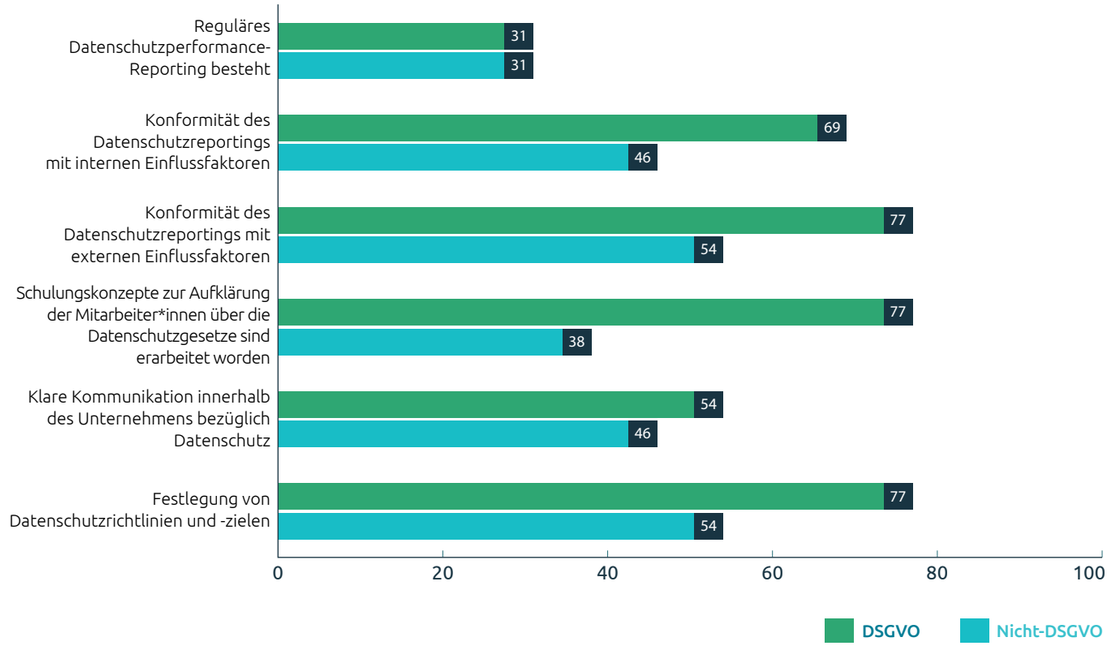
Während bei drei Viertel der Unternehmen die Führungskräfte Schulungskonzepte zur Aufklärung der Mitarbeiter*innen über die Datenschutzgesetze im DSGVO-Kontext umsetzen konnten, ist dieses Engagement im Bereich des Nicht-DSGVO-Kontexts geringer: Hier geben nur 42% der Führungskräfte an, entsprechende Aufklärungsarbeit zu leisten.

Weiterhin gibt jedes zweite Unternehmen im Nicht-DSGVOKontext an, dass die Führungskräfte Führungsstärke in der Einhaltung interner Faktoren wie Unternehmensrichtlinien und -verfahren, Verwaltungsentscheidungen und vertraglichen Anforderungen zeigen. Gleichzeitig berichten 58% der Unternehmen im Nicht-DSGVO-Kontext, dass sich die Führungskräfte dafür einsetzen, die Anforderungen an externe Faktoren wie Datenschutzgesetze, Regierungsvorschriften und Gerichtsentscheidungen einzuhalten. Daraus resultiert ein Widerspruch, da im Unternehmensumfeld den internen Faktoren eine höhere Relevanz zugeordnet wurde, die Führungskräfte sich jedoch tendenziell mehr für die externen Faktoren einsetzen.

Zusammenfassend fällt auf, dass ein fehlendes Verständnis des Leaderships zum Thema Datenschutz die Kultur einer Organisation negativ beeinflussen kann, da die Führungsebene mit einer Vorbildfunktion agiert und die Umsetzung datenschutzrechtlicher Konzepte erfolgreich begleiten sollte. Im Rahmen dieser Studie zeigt sich, dass die Führungskräfte, abgesehen vom Thema des Datenschutz-Reportings, Führungsstärke im Hinblick auf DSGVO-Themen aufweisen. Das Engagement für Nicht-DSGVO-Themen ist hingegen noch ausbaufähig.

Diagramm 3:

Wie zeigt die Top-Managementebene Führungsstärke und Engagement in Bezug auf den Schutz personenbezogener Daten?



Die nachhaltige Etablierung von Datenschutz-Compliance lohnt sich auch finanziell: Die Kosten einer Nicht-Compliance sind mehr als doppelt so hoch wie die Kosten zur Einhaltung der Compliance. Auch sind die Kosten der Compliance-Schaffung industrieabhängig. Vergleicht man das Gesundheitswesen mit der Finanzbranche, sind die Kosten für die Compliance in der Finanzbranche knapp 60% höher, obwohl im Gesundheitswesen mit hochsensiblen Daten umgegangen wird.

Nur jedes sechste befragte Unternehmen besitzt ein gut ausgeprägtes Verständnis der Risikobewertung in Drittstaaten

Erhebung und Verarbeitung

Eine Verarbeitungstätigkeit – das Erheben oder Weiterverarbeiten von personenbezogenen Daten – ist stets der Auslöser und Grund für eine Vielzahl datenschutzrechtlicher Aktivitäten. Im Zuge der DSGVO haben sich viele Abläufe und Maßnahmen etabliert, welche personenbezogene Daten bei der Erhebung und Verarbeitung schützen. Sobald sich Verarbeitungstätigkeiten jedoch (teilweise) in Nicht-DSGVO-Jurisdiktionen verlagern, wird der Schutz personenbezogener Daten deutlich komplexer und es können sogar Widersprüche zwischen datenschutzrechtlichen Vorgaben unterschiedlicher Länder auftreten. Hinzu kommt, dass personenbezogene Daten in Nicht-DSGVO-Ländern mitunter anders definiert werden und sich auch die Definition besonderer Kategorien personenbezogener Daten (sensible Daten) unterscheiden.

Unternehmen müssen daher sicherstellen und dokumentieren, dass auch die Verarbeitung von Daten aus Nicht-DSGVOLändern auf der Grundlage der geltenden Rechtsprechung sowie klar definierten und legitimen Zwecken erfolgt. Insbesondere sollten Betroffene den Zweck, zu dem ihre personenbezogenen Daten verarbeitet werden, verstehen. Ohne eine klare Information über den Zweck der Verarbeitung kann keine angemessene Einwilligung durch eine betroffene Person erfolgen. Deshalb sind Einwilligungserklärungen ein Aspekt, der sich in Nicht-DSGVO-Ländern teilweise sehr stark von der DSGVO unterscheidet.

Angesichts zunehmender Komplexität durch Anforderungen aus Nicht-DSGVO-Ländern haben wir uns die Frage gestellt, wie deutsche Unternehmen ihren eigenen Reifegrad im Hinblick auf die Erhebung und Verarbeitung personenbezogener Daten einschätzen.

Die teilnehmenden Unternehmen zeigen ein schwach ausgeprägtes Verständnis der beiden Prozesse Datenschutz-Folgenabschätzung und Datenschutz-Risikoabschätzung im Nicht-DSGVO-Kontext. Nur 17% der Unternehmen sind der Meinung, dass die Datenschutz-Folgenabschätzung intern gut ausgeprägt ist. Bei der Datenschutz-Risikoabschätzung sind es nur 8%. Im DSGVO-Kontext geben die befragten Unternehmen zur Datenschutz-Folgenabschätzung einen Wert von 83% und zum Datenschutz-Risikomanagement immerhin 67% an. Eine Beibehaltung des aktuellen niedrigen Wissenstands der beiden Prozesse kann weitreichende Konsequenzen für das jeweilige Unternehmen mit sich bringen. Neben Bußgeldern wird auch ein Image- beziehungsweise Reputationsverlust die Geschäftstätigkeit des betreffenden Unternehmens langfristig betreffen.

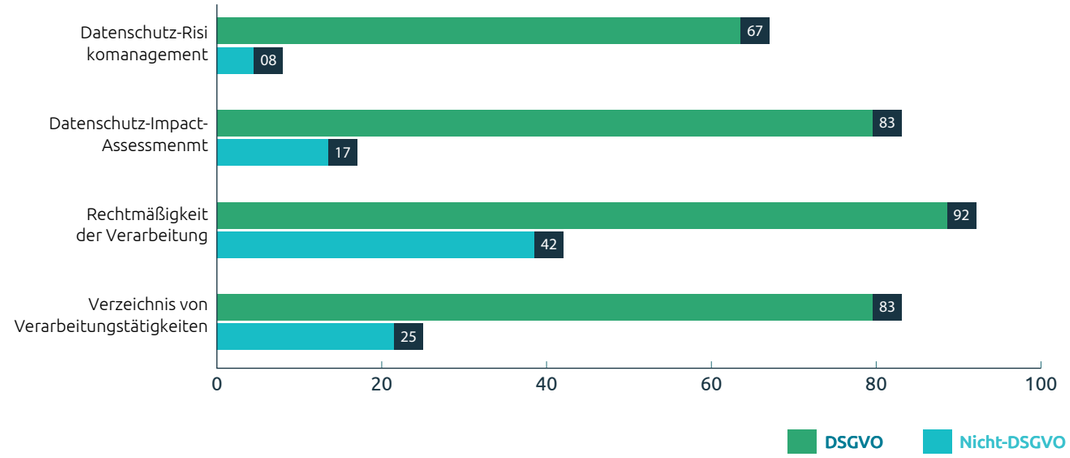
Der Vergleich mit der österreichischen Partnerstudie verdeutlicht, dass in der Datenschutz-Folgenabschätzung ein Drittel der befragten österreichischen Unternehmen ein ausgeprägtes bis sehr ausgeprägtes Verständnis besitzen.

Zusätzlich zu den zwei zuvor genannten Prozessen besitzt knapp die Hälfte der deutschen Unternehmen ein ausgeprägtes oder sehr ausgeprägtes Wissen über die Rechtmäßigkeit der Verarbeitung im Nicht-DSGVO-Kontext. Beim Verzeichnis von Verarbeitungstätigkeiten schätzen lediglich 25% der Antwortenden ihr Wissen als ausgeprägt oder sehr ausgeprägt ein. Die Verteilung der Selbsteinschätzung mit DSGVO-Richtlinien ist weitaus ausgeprägter als im drittstaatlichen Kontext. Hier gehen 93% von (sehr) ausgeprägten Kenntnissen zur Rechtmäßigkeit der Verarbeitung aus. Das Niveau des Verzeichnisses von Verarbeitungstätigkeiten und der Datenschutz-Folgenabschätzung geben jeweils 83% mit ausgeprägt / sehr ausgeprägt an. Der Punkt des Datenschutz-Risikomanagements ist auch bei der DSGVO auf dem hinteren Platz mit lediglich 63%.

Kurzum: Durch die Beachtung der zuvor genannten Aspekte des Datenschutzes im Kontext der Erhebung und Verarbeitung können Unternehmen das Vertrauen ihrer Kund*innen und Geschäftspartner*innen stärken und das Risiko von Verstößen gegen Datenschutzbestimmungen minimieren, was wiederum zu einem besseren Geschäftsergebnis führen kann. Die Studie zeigt, dass ein großer Anteil der außerhalb des Geltungsbereichs der DSGVO tätigen Unternehmen hier deutlichen Handlungsbedarf hat.

Diagramm 4:

Wie viele der befragten Unternehmen bewerten folgende Prozesse als ausgeprägt oder sehr ausgeprägt?



Aufsichtsbehörden können aus den unterschiedlichsten Gründen aktiv werden und Prüfungen initiieren. Besonders spannend ist dabei die Rolle von Landesgrenzen. So löste eine Verkehrskontrolle der österreichischen Polizei im Jahr 2019 die Prüfung einer deutschen Aufsichtsbehörde bei einem deutschen Automobilhersteller aus, welche 2022 in einem Bußgeld in Höhe von EUR 1,1 Millionen resultierte. Auch ein norwegisches Mautunternehmen geriet in den Fokus der eigenen Aufsichtsbehörde, nachdem in einem Fernsehbeitrag über Datentransfers nach China berichtete wurde. Die nachfolgende Prüfung ergab für die Behörde, dass Daten unrechtmäßig übermittelt wurden und für das Unternehmen ein festgesetztes Bußgeld in Höhe von umgerechnet knapp EUR 500.000 verhängt wurde.

Bei jedem zweiten befragten Unternehmen fehlen Maßnahmen zur Aufklärung der Datenverarbeitung in Drittstaaten

Betroffene Personen und Behörden

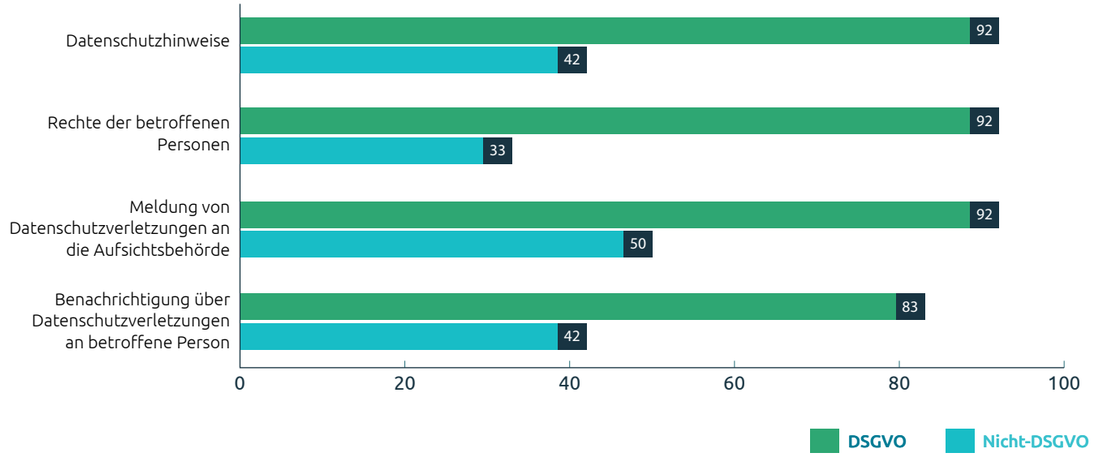
Unternehmen, die personenbezogene Daten verarbeiten, sind gemäß DSGVO und vielen weiteren Datenschutzgesetzen in Nicht-EU-Ländern dazu verpflichtet, betroffene Personen umfassend über die Verarbeitung ihrer Daten zu informieren. Die Umsetzung der Informationspflichten zählt zu den wichtigsten datenschutzrechtlichen Aufgaben und hat eine große Außenwirkung. Nicht umgesetzte Informationspflichten stellen einen Datenschutzverstoß dar und können neben Bußgeldern auch erhebliche Reputationsschäden nach sich ziehen. Nicht nur den Betroffenen, sondern auch gegenüber den jeweiligen Aufsichtsbehörden sind Unternehmen auskunftspflichtig. Auch wenn die DSGVO für viele Nicht-EU-Länder als richtungsweisend gilt, kann es zu großen Abweichungen kommen. Beispielsweise sind Unternehmen in Kolumbien dazu verpflichtet, zwei Mal im Jahr der Aufsichtsbehörde die Anzahl eingegangener Betroffenenrechteanfragen zu übermitteln. Die kalifornische Datenschutzregelung, die aus dem California Consumer Privacy Act (CCPA) und dessen Erweiterung, dem California Privacy Rights Act (CPRA) hervorgeht, verlangt von Unternehmen, bestimmte Informationen über die Bearbeitung von Betroffenenrechteanfragen offenzulegen. Darunter fallen die Anzahl der abgelehnten Betroffenenrechteanfragen und die durchschnittliche Bearbeitungsdauer. Informationspflichten sind vielseitig und können bei Verstößen ernstzunehmende Konsequenzen nach sich ziehen. Gerade deshalb sollten sich Unternehmen auch mit den rechtlichen Anforderungen in Nicht-EU-Ländern stärker auseinandersetzen. Daher haben wir uns die Frage gestellt, ob deutsche Unternehmen diesen Herausforderungen gewachsen sind.

Die Ergebnisse der Befragung zeigen, dass in allen vier untersuchten Maßnahmen (Datenschutzhinweise, Rechte der betroffenen Person, Meldungen von Datenschutzverletzungen an die Aufsichtsbehörde und Benachrichtigung über Datenschutzverletzungen an die betroffene Person) maximal 50% der Teilnehmenden angeben, dass die jeweilige Maßnahme im Unternehmen im Nicht-DSGVO-Kontext entweder ausgeprägt oder sehr ausgeprägt ist: Die größte Zustimmung mit 50% erfährt die Meldung von Datenschutzverletzungen an die Aufsichtsbehörde; hingegen sehen nur 33% die Rechte der betroffenen Personen als implementiert an. 42% der Befragten sehen die anderen beiden Maßnahmen als ausgeprägt oder sehr ausgeprägt an.

Ein deutlicher Unterschied zeigt sich bei den identischen Maßnahmen im Kontext der DSGVO: Im Durchschnitt haben doppelt so viele der befragten Unternehmen eine erfolgreiche Umsetzung hinsichtlich ihrer datengetriebenen Verpflichtungen gegenüber Personen und Behörden erreicht. Bei der Benachrichtigung über Datenschutzverletzungen an die betroffene Person geben 83% und bei den weiteren drei Maßnahmen sogar jeweils 92% der Befragten an, die Maßnahmen seien ausgeprägt oder sehr ausgeprägt. Es ist zu betonen, dass die DSGVO zu den ersten und weltweit strengsten Datenschutzregelungen gehört. Verstöße werden hier früher und härter bestraft als in der Mehrheit der Drittländer. Vor diesem Hintergrund lässt sich nachvollziehen, dass bestimmte Maßnahmen einen deutlich höheren Stellenwert genießen als außerhalb der DSGVO. Daher ist die erfolgreiche Implementierung dieser Maßnahmen zwar noch nicht flächendeckend gegeben, jedoch sollten sie keinesfalls vernachlässigt werden, da auch in Drittstaaten die Bedeutung der Datenschutzrechte von Betroffenen zunehmend an Gewicht gewinnt. Wenn betroffene Personen nicht darüber aufgeklärt werden, wie beispielsweise ein System mit ihren Daten verfährt bzw. wie sie verarbeitet werden, kann dies zu Problemen im Consent Management führen. Daher sollten immer angemessene Datenschutzhinweise vorhanden sein, um Nutzer*innen hierüber aufzuklären. Das Fehlen solcher Hinweise kann bei auftretenden Datenschutzverletzungen, etwa durch Hackerangriffe oder ungewollte Weitergabe an Dritte, die Rückverfolgung erschweren, ob die betroffenen Personen vor der ursprünglichen Datenerhebung oder der Verarbeitung ihrer Daten ab einem bestimmten Zeitpunkt zugestimmt haben. In Fällen, in denen der Speicherort der Daten unbekannt ist, gestaltet sich die nachträgliche Löschung oft als schwierig oder unmöglich. Um solche Fälle zu vermeiden, ist die Umsetzung der angesprochenen Maßnahmen gegenüber Betroffenen wichtig, vor allem für den Vertrauensaufbau und ein größeres Sicherheitsgefühl. Da das Wissen und die Umsetzung im DSGVO-Bereich schon weit fortgeschritten sind, ist anzunehmen, dass ein Grundstein für eine erfolgreiche Handhabung der vier Methodiken gelegt ist und in den kommenden Jahren auch entsprechend im Nicht-DSGVO-Bereich ausgebaut werden kann.

Diagramm 5:

Wie viele der befragten Unternehmen schätzen folgende Maßnahmen, mit Bezug auf die Verpflichtungen gegenüber betroffenen Personen und Behörden, als ausgeprägt oder sehr ausgeprägt ein?



Unternehmen verletzen immer wieder Informationspflichten. Eine spanische Großbank wurde 2020 zu einer Geldstrafe von EUR 5 Millionen verurteilt, da in ihren Datenschutzhinweisen nicht ordnungsgemäß erläutert wurde, wie die Bank die personenbezogenen Daten ihrer Kunden erhebt und verarbeitet. Auch hat die Bank Kundendaten für Verarbeitungstätigkeiten ohne Zustimmung der betroffenen Personen genutzt. In einem anderen Fall wurde eine Geldstrafe in der Höhe von EUR 6 Millionen gegen eine weitere spanische Großbank verhängt, da die spanische Aufsichtsbehörde in den Datenschutzhinweisen Widersprüche festgestellt hat. Zudem wurden die Datenschutzhinweise zu vage formuliert, sodass Einwilligungen nicht DSGVO-konform erfolgt sind.

Nur knapp über die Hälfte der befragten Unternehmen erfüllt bereits heute Privacy by Design/Default Prinzipien gemäß DSGVO

Privacy by Design/Default

Privatsphäre zu einem integralen Bestandteil der eigenen Organisation, ihrer Prozesse und insbesondere von IT-Systemen zu machen stellt eine der größten Herausforderungen im Datenschutz dar. Dafür müssen Datenschutzprinzipien verinnerlicht werden, sodass diese auch bei der Gestaltung von Produkten und Services standardmäßig Anwendung finden und nicht kurzfristigen Geschäftsinteressen untergeordnet werden. Im Gegensatz zu Betroffenenrechten oder Informationspflichten ist Privacy by Design/Default kein Impuls, der von außen kommt. Proaktives Handeln ist notwendig, um Datenschutz hier nachhaltig zu etablieren.

Privacy by Design/Default soll in erster Linie eine Klammer um Einzelmaßnahmen bilden, damit Prinzipien und Anforderungen des jeweiligen Datenschutzgesetzes eingehalten werden können. Um Datenschutz sicherzustellen und Privatsphäre zu ermöglichen, müssen alle Produkte und Services von der Erhebung bis zur Löschung personenbezogener Daten einen ganzheitlichen Ansatz verfolgen. Diverse technische und organisatorische Maßnahmen können Privacy by Design/Default sicherstellen, weshalb es, Stand heute, keinen einheitlichen Ordnungsrahmen gibt. Da Maßnahmen stets entsprechend der durchzuführenden Verarbeitungstätigkeit und Rahmenbedingungen definiert werden, haben wir uns die Frage gestellt, wie deutsche Unternehmen dieser Herausforderung im heimischen und internationalen Markt begegnen.

In der durchgeführten Studie gaben 42% der befragten Unternehmen an, dass ein Konzept für Privacy by Design/Default in ihrem Unternehmen im Nicht-DSGVO-Kontext ausgeprägt oder sehr ausgeprägt ist. Dadurch laufen mehr als die Hälfte der befragten Unternehmen Gefahr, eine potenzielle nachträgliche Datenfilterung vornehmen zu müssen, um die erhobenen Daten auf das Minimum zu reduzieren. Durch diesen Ansatz leidet nicht nur die interne Prozesseffizienz, sondern auch das Kundenvertrauen kann dadurch geschwächt werden.

Im DSGVO-Kontext liegt die Implementierung eines Ansatzes für Privacy by Design/Default mit 58% nur unwesentlich höher. Unternehmen sollten die Bedeutung von Privacy by Design/Default erkennen und beispielsweise geplante oder bestehende Onlineportale, Websites und Anwendungen mit verbesserten Datenschutzfunktionen ausstatten.

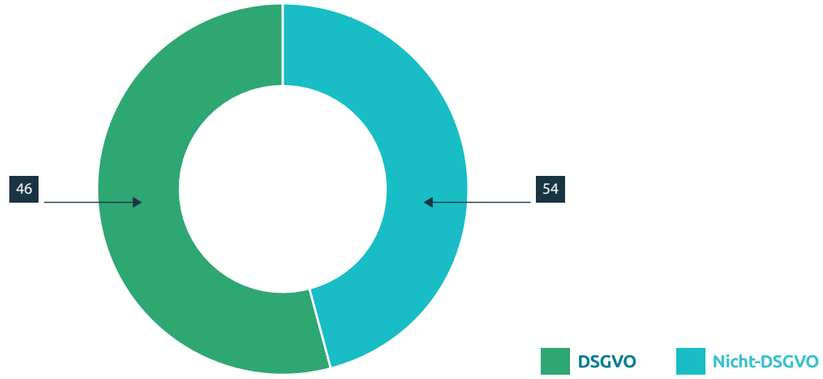
Da die Entwicklung eines Konzepts für Privacy by Design/Default für viele Unternehmen auf den ersten Blick sehr umfangreich wirkt, setzen wir auf Best Practices, um eine einfachere Implementierung zu gewährleisten. Beispielsweise kann ein Privacy Impact Assessment potenzielle Risiken in der Privatsphäre schon beim Design einer Applikation oder eines Services identifizieren. Werden gewisse Risiken frühzeitig festgestellt, gilt es im Anschluss technologische Lösungen und Prozesse zu implementieren, um diese abzufedern.

Des Weiteren sollte es für Betroffene nachvollziehbar sein, wer die Ansprechpersonen im Unternehmen sind, falls sie Fragen zum Erhebungs- und Speicherungskonzept ihrer Daten haben. Dadurch wird schon während der Designphase einer Applikation oder eines Services eine offene Kommunikation und Transparenz gefördert. Dies führt zu positiven Auswirkungen auf das Bewusstsein der Kund*innen, da sie dem Unternehmen gegenüber mehr Vertrauen entgegenbringen können.

Alles in allem ist ein Privacy by Design/Default-Ansatz nicht nur wichtig, um interne Prozesse in der Datenspeicherung und -verarbeitung effizienter zu gestalten, sondern auch essenziell, um Compliance-Anforderungen gerecht zu werden sowie gegenüber den Betroffenen die Sicherstellung der Privatsphäre ihrer Daten zu gewährleisten.

Diagramm 6:

Wie viele der befragten Unternehmen finden, dass die Erhebung und Verarbeitung personenbezogener Daten auf das für den angegebenen Zweck erforderliche Maß ausgeprägt oder sehr ausgeprägt ist?



Was passieren kann, wenn Privacy by Design/Default nicht nachhaltig umgesetzt wird, zeigt das Beispiel einer US-amerikanischen Hotelkette. Durch einen Cyberangriff wurden die personenbezogenen Daten von über 30 Millionen EU-Bürger*innen gestohlen. Die Untersuchung des Information Commissioner's Office (ICO) in Großbritannien ergab, dass die technischen und organisatorischen Maßnahmen nicht geeignet waren, um den Schutz der personenbezogenen Daten sicherzustellen. Daraus resultierte ein Bußgeld in Höhe von EUR 20 Millionen.

Über 60% der Unternehmen verfügen über einen nur geringen Reifegrad bei der grenzüberschreitenden Datenübermittlung

Weitergabe, Übertragung und Offenlegung

Unternehmen stehen vor besonderen Herausforderungen, wenn personenbezogene Daten an europäische Auftragsverarbeiter oder gar in Drittstaaten transferiert werden. Die Übermittlung gemäß DSGVO ist bereits umfangreich reguliert, jedoch steigt die Komplexität, wenn auch das Empfängerland Vorgaben zum Rücktransfer der Daten macht.

Gemäß DSGVO dürfen personenbezogene Daten nur in Drittländer übermittelt werden, die ein angemessenes Schutzniveau bieten. Seitens der europäischen Kommission werden Drittstaaten fortlaufend auf ihr Schutzniveau geprüft. Dies deckt jedoch nur die europäische Perspektive eines internationalen Datentransfers ab. Vor diesem Hintergrund haben wir uns die Frage gestellt, welche Maßnahmen deutsche Unternehmen für die Weitergabe, Übermittlung und Offenlegung von personenbezogenen Daten ergreifen und wie ausgeprägt diese in den jeweiligen Organisationen wahrgenommen werden. Bevor Daten an Dritte und in andere Länder weitergegeben werden können, müssen sogenannte Auftragsverarbeitungsverträge mit potenziellen Dienstleistern geschlossen werden. Diese legen im Detail fest, wie der Auftragsverarbeiter personenbezogene Daten von Kund*innen verarbeiten darf und welche technischen und organisatorischen Maßnahmen getroffen werden. Dieser Prozess wurde in der durchgeführten Befragung von allen teilnehmenden Unternehmen im DSGVO-Kontext mit 100% bewertet. Dies zeigt, dass innerhalb der EU für diese Art von Datenbeschaffung und -verarbeitung sehr strenge Regularien gelten, welche im Detail bereits von Unternehmen beachtet werden. Im Nicht-DSGVO-Kontext geben 58% der befragten Unternehmen an, dass die Qualität ihrer Maßnahmen für eine rechtskonforme Auftragsverarbeitung ausgeprägt bis sehr ausgeprägt ist.

Die anderen beiden in dieser Studie erhobene Prozesse sind die grenzüberschreitende Datenübermittlung und die Datenlokalisierung/-residenz. Wenn bei der Datenlokalisierung/-residenz die Erstellung und Erhebung von Daten in einer spezifischen geographischen Region erfolgt, dann muss auch die Verarbeitung der Daten in dieser geographischen Region geschehen. Dadurch können Unternehmen, die in einem bestimmten Land oder Region tätig sind, gesetzlich verpflichtet sein, die Daten ihrer Nutzer*innen oder Kund*innen in diesem Land oder dieser Region zu speichern. Der Zweck der Datenlokalisierung/-residenz ist es, sicherzustellen, dass die Daten weiterhin den Gesetzen und Vorschriften des Landes oder der Region unterliegen, in dem oder in der sie erhoben wurden.

Die Relevanz dieses Prozesses nimmt besonders durch die kontinuierliche Verbreitung des Cloud Computings zu. Cloud-Service-Provider betreiben häufig Datenzentren in anderen (Dritt-)Ländern anstelle ihres Heimatstandorts, was diese Thematik zusätzlich an Bedeutung gewinnen lässt. Hier ist für Unternehmen bei der Auswahl eines passenden Dienstleistenden besondere Sorgfalt geboten, da sonst eine unrechtmäßige Übermittlung in ein Drittland droht. Wenn Unternehmen die Daten in einer bestimmten Region speichern müssen, kann es schwieriger sein, diese Daten in ein Drittland zu übertragen. In vielen Fällen besteht das Problem darin, dass das Zielland für die Datenübermittlung nicht die gleichen Datenschutzstandards wie das Herkunftsland aufweist. Dadurch sind die übermittelten Daten potenziellen Sicherheitsrisiken ausgesetzt, und die Vertraulichkeit sowie der Schutz der Daten können nicht mehr gewährleistet werden.

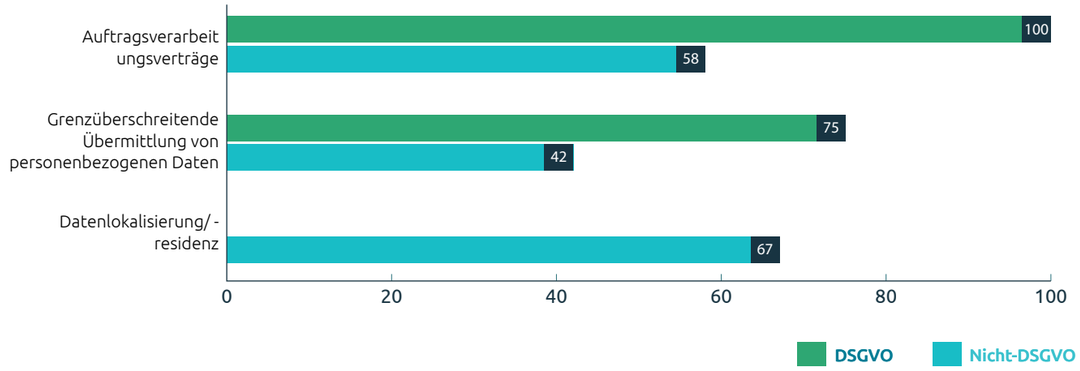
Aus diesem Grund ist die Datenübermittlung in Drittländer im Allgemeinen aus vielen Gründen noch komplexer als die Datenlokalisierung/-residenz. Dieser Ansatz spiegelt sich auch in den Ergebnissen der Studie wider: 42% der befragten Unternehmen sind der Meinung, dass ihre Prozesse zur grenzüberschreitenden Datenübermittlung im Nicht-DSGVO-Kontext ausgeprägt oder sehr ausgeprägt sind. Bei der Datenlokalisierung/-residenz sind es 67%.

Dies zeigt, dass das Verständnis einer Übermittlung ins Ausland als ein sehr wichtiger Ansatzpunkt betrachtet werden muss. Durch verschiedene Online-Datenspeicherungsdienste oder Cloud-Dienstleister kann nicht immer gewährleistet werden, dass die Daten auch in dem Land bleiben, in dem sie erhoben wurden.

Die mit der Übermittlung verbundenen rechtlichen, regulatorischen und sicherheitsrelevanten Fragen sollten keineswegs unterschätzt werden. Unternehmen müssen diese Fragen sorgfältig abwägen, bevor sie Daten in ein Drittland übermitteln. Dies dient dazu, die Einhaltung der Vorschriften zu gewährleisten und die mit der Datenübermittlung verbundenen Risiken und potenziellen Strafen der Nichteinhaltung zu minimieren.

Diagramm 7:

Wie viele der befragten deutschen Unternehmen schätzen den Reifegrad der folgenden Prozesse als ausgeprägt oder sehr ausgeprägt ein?



Im Jahr 2021 stellte die schwedische Datenschutzbehörde bei einem schwedischen Online-Zahlungsdienstleister fest, dass das Unternehmen keine Angaben dazu machen konnte, in welche Länder außerhalb der EU/des EWR personenbezogene Daten übermittelt werden oder wie und wo Einzelpersonen Informationen zu den Mechanismen der Datenübermittlung in Drittländer erhalten können. Dies stellt eine Verletzung des Grundprinzips der Transparenz sowie des Informationsrechts der betroffenen Personen dar und führte zu einer Verhängung einer Geldstrafe von über EUR 700.000.

Herausforderungen aus Unternehmenssicht

Kein rechtskonformer internationaler Datentransfer ohne Verständnis von Nicht-DSGVO-Richtlinien

Ziel der in Deutschland ansässigen, außerhalb der EU tätigen Unternehmen sollte ein erfolgreich umgesetztes Konzept zum Thema Datenschutz sein. Da, wie in den vorherigen Kapiteln besprochen, eine geschäftliche Tätigkeit mit Drittstaaten einige nicht außer Acht zu lassende Risiken mit sich bringt, wenn die jeweiligen lokalen Datenschutzregelungen nicht korrekt befolgt werden. Deshalb sollte sich jedes Unternehmen in detaillierter Weise damit auseinandersetzen. Gleichzeitig wird bislang die Implementierung entsprechender Vorhaben nicht immer vollständig umgesetzt. Daher sollten die Teilnehmer*innen in der abschließenden Phase der Befragung aus zehn potenziellen Herausforderungen, die sich auf die unternehmensinterne Einhaltung von Vorschriften aus Nicht-EU/EWR-Ländern beziehen, die fünf wichtigsten auswählen und diese auf einer Skala von 1 bis 5 bewerten.

Demnach ergab sich die größte Herausforderung in der Kenntnis der Nicht-DSGVO-Vorschriften und Verständnis ihrer Relevanz oder Anwendbarkeit. Diese Herausforderung ist von besonderer Bedeutung, da zunächst ein fundiertes Grundwissen über die Vielfalt an datenschutzrechtlichen Regelungen aufgebaut werden muss, damit man potenzielle Konflikte oder gar rechtliche Konsequenzen verstehen und diese dadurch vermeiden kann. Eine angemessene Berücksichtigung der Anwendbarkeit der einzelnen Vorschriften ist von großer Bedeutung, da sich einige Bestimmungen möglicherweise zwischen Ländern ähneln, aber in Details dennoch unterscheiden.
Die zweitgrößte Herausforderung liegt in der Bewältigung der Vielfalt der relevanten und anwendbaren Vorschriften, was sich mit dem vorherigen Punkt überschneidet. Es ist nicht nur von Bedeutung, die verschiedenen Vorschriften zu kennen, sondern auch zu verstehen, wie mit ihnen umgegangen werden kann und an welchem Punkt beispielsweise die datenschutzrechtlichen Regelungen greifen. Aufbauend darauf wurde als drittgrößte Herausforderung das Verständnis des Vorschriftenumfangs und der erforderlichen Maßnahmen genannt.

Diese drei Herausforderungen gehen Hand in Hand, da insbesondere das Verständnis und der Umgang mit Nicht-DSGVO-Vorschriften als problematische Aspekte betrachtet werden. In der durchgeführten Studie in Österreich ergab sich im letzten Befragungsabschnitt eine Übereinstimmung mit den drei top-priorisierten Herausforderungen in Deutschland. Diese Ergebnisse legen nahe, dass die genannten Hindernisse als relevant für Deutschland und Österreich betrachtet werden können und keinesfalls unterschätzt werden sollten.

Um diesen Herausforderungen langfristig zu begegnen, empfiehlt es sich als ersten Schritt, eine umfassende Bestandsaufnahme durchzuführen, um die spezifischen Bereiche zu identifizieren, in denen grundlegendes Wissen über Nicht-DSGVO-Vorschriften fehlt. Anschließend kann gezielt in diesen Bereichen angesetzt werden. Dies ermöglicht es den Mitarbeiter*innen, Überforderung zu vermeiden und schrittweise vorzugehen. Eine weitere mögliche Unterstützung besteht darin, die Bereiche zu erfassen, in denen bereits ein solides Verständnis im Kontext der DSGVO aufgebaut wurde. Dieses vorhandene Wissen erleichtert den Einstieg in den Nicht-DSGVO-Kontext erheblich.

Im Abschnitt „Erhebung und Verarbeitung" weist der Reifegrad des Verzeichnisses für Verarbeitungstätigkeiten bei 25% der Unternehmen, die zusätzlich den Datenschutzrichtlinien außerhalb der EU unterliegen, eine positive Quote auf. Die Steigerung dieses Wertes ist von besonderer Bedeutung, da das Verzeichnis eine umfassende Übersicht und Dokumentation über Verfahren bietet, in denen personenbezogene Daten verarbeitet werden. Es ermöglicht eine präzise Erfassung der gesammelten und verarbeiteten Daten, was wiederum zu einem besseren Verständnis der Abläufe beiträgt. Dieses Verständnis kann genutzt werden, um spezifische Vorschriften im Rahmen der DSGVO zu identifizieren und das gewonnene Wissen auf potenzielle Anwendungsbereiche außerhalb des DSGVO-Kontexts zu übertragen. Des Weiteren existieren weltweit viele verschiedene Länder mit unterschiedlichen Vorschriften zum Datenschutz. Bei der Berücksichtigung aller bestehenden Regularien kann häufig eine Überforderung aufgrund der Fülle an Informationen entstehen. Falls das eigene Unternehmen nur mit einigen bestimmten Ländern im Bereich der Datenerhebung, des Datentransfers und der Datenverarbeitung kooperiert, sollte der Umfang eingegrenzt und sich auf die Vorschriften dieser Länder fokussiert werden. Bei der Zusammenarbeit mit Kunden in Kanada beispielsweise ist ein fundiertes Verständnis der PIPEDA, der kanadischen Datenschutzgrundverordnung, unerlässlich. Hingegen sind Kenntnisse der Gesetze eines anderen Landes, die keinen direkten Einfluss auf die Aktivitäten in Kanada haben, in diesem Zusammenhang nicht erforderlich und könnten unter Umständen zu Verwirrung führen.

Die zwei verbleibenden Herausforderungen aus der Befragung grenzen sich inhaltlich ab: In diesem Zusammenhang liegt der Fokus eher auf der Implementierung von Lösungen innerhalb des Unternehmens als auf dem grundlegenden Verständnis der Vorschriften und des Kontexts. Die Mobilisierung aller relevanten Stakeholder zur Umsetzung von Maßnahmen zur Einhaltung von Nicht-DSGVO-Vorschriften wurde als die viertwichtigste Priorität bewertet. An fünfter Stelle wurde das Aufrüsten bestehender technischer DSGVO-Lösungen genannt, um auch Nicht-DSGVO-Vorschriften zu erfüllen. Bei diesen beiden Herausforderungen ist vor allem die Top-Führungsebene gefordert, um die Datenschutzkultur im Unternehmen zu entwickeln und deren Bedeutung zu vermitteln. Dabei sollte der Fokus gezielt auf relevante Nicht-DSGVO-Vorschriften gelegt werden, da die Befragung zeigt, dass insbesondere in diesem Bereich Wissen und Bewusstsein fehlen. Die Etablierung einer erfolgreichen Datenschutzkultur wird maßgeblich durch eine aktivere Beteiligung der Top-Führungsebene und anderer relevanter interner Stakeholder sowie durch die Schaffung von Möglichkeiten für Mitarbeiter*innen, ein besseres Verständnis für die Einhaltung von Nicht-DSGVO-Vorschriften zu entwickeln, gelegt. Gegebenenfalls können Schulungen oder Workshops über Compliance mit Nicht-DSGVO-Lösungen unterstützen.

Abschließend kann die Aufrüstung bestehender technischer DSGVO-Lösungen in Gang gesetzt werden, indem etwa die Datensicherheit hinsichtlich der Speicherung und Übertragung auf den neusten Stand gebracht wird. Aktuell haben 19% der gesamten Unternehmen keinerlei Maßnahmen zur Weitergabekontrolle der Daten getroffen. Dies hat zur Folge, dass sensible personenbezogene Daten oft unverschlüsselt versendet werden und bei der Übermittlung von Unbefugten eingesehen oder verarbeitet werden können. Es gilt, Gegenmaßnahmen nicht nur im DSGVO-Kontext, sondern auch außereuropäisch zu implementieren, um das notwendige technische Grundgerüst zu besitzen, welches zu einem erfolgreichen Datenschutzkonzept beiträgt.

Diagramm 8:

Was sind die fünf größten Herausforderungen, wenn es um die Einhaltung von Nicht-DSGVO-Vorschriften geht?

Unser Fazit

Die Bedeutung von internationalem Datenschutz darf von deutschen Unternehmen nicht unterschätzt werden

Die vorliegende Studie hat gezeigt, dass deutsche Unternehmen bei ihrer Geschäftstätigkeit in Drittstaaten mit besonderen Herausforderungen im Datenschutz konfrontiert sind. Die DSGVO hat zwar den Datenschutz innerhalb der EU reguliert und europäischen Bürger*innen mehr Kontrolle über ihre personenbezogenen Daten gegeben, jedoch haben weltweit immer mehr Länder außerhalb der EU eigene Datenschutzbestimmungen erlassen. In vielen Fällen haben diese Bestimmungen auch eine extraterritoriale Wirkung und können somit auch für Unternehmen in Deutschland Anwendung finden, sofern personenbezogene Daten innerhalb oder außerhalb von Drittstaaten verarbeitet werden. Die Analyse und Ausarbeitung der Studie zeigt, dass in Bezug auf außereuropäische Datenschutzregulierungen bereits ein gewisses Grundverständnis vorhanden ist, welches aber noch ausbaufähig ist. Der aktuelle Kenntnisstand dürfte die Unternehmen nicht hinreichend vor weitreichenden Konsequenzen schützen.

Um den korrekten Umgang mit internationalen Datenschutzanforderungen sicherzustellen, kann eine gute DSGVO-Compliance helfen. Eine nachhaltige Datenschutzorganisation erfordert eine gelebte Datenschutzkultur sowie einen hohen Reifegrad etablierter Datenschutz-Compliance Maßnahmen. Schulungen und Trainingsmaßnahmen für Mitarbeiter*innen können dazu beitragen, das Bewusstsein für Datenschutz- und Sicherheit zu erhöhen. Ein gesteigertes Bewusstsein für die erforderlichen Kenntnisse erleichtert nicht nur die aktive Übernahme einer Vorbildrolle durch die Top-Führungsebene gegenüber den Mitarbeiter*innen, sondern fördert auch die erfolgreiche Etablierung von Compliance-Prozessen, einschließlich des Umgangs mit Betroffenen bei Nichteinhaltung von Datenschutzvorschriften. Präventive Maßnahmen können dazu beitragen, Konsequenzen wie beispielsweise einen Image- oder Vertrauensverlust des Unternehmens sowie einen negativen Einfluss auf die Geschäftsfähigkeit zu verhindern.

Die Untersuchung hat auch gezeigt, dass die Erfüllung der lokalen Datenschutzbestimmungen eine erhebliche Herausforderung für die Unternehmen darstellt, da in jedem Land unterschiedliche Datenschutzbestimmungen gelten. Dies ist unter anderem darauf zurückzuführen, dass Datenschutzregelungen in vielen Drittstaaten im Vergleich zur DSGVO noch relativ neu sind. Aus diesem Grund fehlt vielen Privatpersonen, Unternehmen sowie Behörden der Überblick und das Wissen über die Ausübung ihrer Rechte oder die Grenzen, die für Unternehmen bei der Verarbeitung und Weitergabe von Daten gelten. Zudem werden Nicht-DSGVO-Richtlinien von Unternehmen aktuell, laut unseren Studienergebnissen, als weniger wichtig im Vergleich zur DSGVO erachtet. Da die Bedeutung des Themas Datenschutz in den letzten Jahren aber zugenommen hat, wachsen das Bewusstsein für und das Wissen über Nicht-DSGVO-Richtlinien. Die bestehenden Wissenslücken im Vergleich zur DSGVO sind teilweise noch erheblich, lassen sich aber in Teilen durch das frühere Inkrafttreten der DSGVO erklären. Es ist daher von enormer Bedeutung, dass Unternehmen die lokalen Regelungen verstehen, sich frühzeitig mit den verschiedenen Verordnungen auseinandersetzen und kontinuierlich auf dem neuesten Stand bleiben.

Um dem aktuellen Kenntnisstand im Nicht-DSGVO-Bereich weiter auf die Sprünge zu helfen und bestehenden Herausforderungen entgegenzutreten, wurden in dieser Studie auch mehrere Handlungsempfehlungen thematisiert. Diese sollen deutsche Unternehmen auf dem Weg zu globalen datenschutzrechtlichen Experten unterstützen. So helfen beispielsweise Privacy Impact Assessments bereits in einem frühen Stadium des Aufbaus eines datenschutzkonformen Services oder einer Applikation hohe Aufwände einer nachträglichen Anpassung an geltende Datenschutzgesetze zu vermeiden. Außerdem vereinfacht eine Bestandsaufnahme bestehender wichtiger Wissenslücken die Struktur des Lernprozesses.

Am wichtigsten, ist jedoch zu betonen, dass die Umsetzung von Nicht-DSGVO Gesetzgebungen nicht von Grund auf neu durchgeführt werden muss und soll. Die bereits solide aufgebaute Datenschutzorganisation unserer Studienteilnehmer und die Anlehnung vieler Nicht-DSGVO Gesetzgebungen an die DSGVO, bietet ein großes Potential für Synergieeffekte. Vor der Umsetzung von Nicht DSGVO-Vorschriften sollten deshalb bestehende Prozesse und Systeme analysiert werden, inwieweit sie an die neuen Vorgaben angepasst werden können.

Insgesamt sollten Unternehmen den Datenschutz als eine kollektive Anstrengung eines gesamten Unternehmens betrachten, um langfristig erfolgreich zu sein. Gleichzeitig sollten sie sich auf Veränderungen einstellen und bereit sein, ihre Geschäftsmodelle und -prozesse an neue Herausforderungen anzupassen.

Wir sind Capgemini Invent

Das Innovations-, Design- und Transformations-Powerhouse der Capgemini-Gruppe

In einer Welt geprägt von Disruption und schnellem Wandel erhöhen sich die Anforderungen an Unternehmen, Transformationschancen zu nutzen und sich ständig neu zu erfinden. Um im lebhaften Wettbewerb bestehen zu können, müssen sie fortlaufend effizienter, resilienter, nachhaltiger und datengetriebener werden. Die globale Pandemie erhöht darüber hinaus den Bedarf an purpose-orientierten Organisationen, die starke Beziehungen zu ihren Kund*innen aufbauen.

Indem wir Strategie, Technologie, Data Science und Creative Design mit einer innovativen Denkweise vereinen, optimieren und transformieren wir kollaborativ mit unseren Kunden ihr Business. Dabei unterstützen wir sie, sich im Markt zu positionieren und den Weg in die Zukunft zu weisen. Von zukunftsorientierten CEOs, strebend nach der nächsten Marktinnovation, bis hin zu CMOs, die das Geschäft neu definieren, arbeiten wir mit CxOs zusammen, um den Weg von der Idee, über den Prototypen bis hin zu skalierbaren Produkten, Dienstleistungen und Erfahrungen zu beschleunigen. Als Teil von Capgemini fordern wir den Status quo heraus, indem wir ihn verändern, Wachstum vorantreiben und unseren Kund*innen dabei helfen, die Zukunft ihrer Unternehmen zu gestalten.

Changing minds, touching hearts, moving markets.
Wir verleihen Ihrer Marke Energie und halten Sie wettbewerbsfähig in Zeiten von Real-Time-Kundenzentrierung. Unsere globalen, multidisziplinären Teams ermöglichen es Ihnen, Ihr Unternehmen neu zu erfinden, Ihre Marke an neue Normen anzupassen, das gesamte Kundenerlebnis zu verbessern und Ihre Zielgruppe mit neuen datengesteuerten Marketingmethoden anzusprechen. Dabei schaffen wir kundenorientierte Abläufe, die Vertrieb, Service, Marketing und Handel vereinen.

Als Teil von Capgemini Invent bietet frog im Rahmen unserer Customer-First-Services marktführende Design-, Innovations- und Markenkompetenz. Wir entwickeln Produkte, Services und Erlebnisse, die für Ihre Kund*innen relevant sind.

Disruptionen sind nicht neu, aber das Tempo nimmt zu.
Wir machen den Wandel möglich. Wir helfen unseren Kunden, sich anzupassen, um agiler, widerstandsfähiger, relevanter und nachhaltiger zu werden. Dies erfordert eine zielgerichtete Strategie, verbesserte, datengesteuerte Geschäftsprozesse, einen Fokus auf die Erfahrung Mitarbeitender, intelligentes Personal und eine Unternehmenskultur sowie eine unterstützende Technologielandschaft. Bei Capgemini Invent vereinen wir eine einzigartige Kombination aus Strategie-, Prozess-, Personal- und Technologie-Know-how mit der Leistungsfähigkeit von Daten, um Ihre End-to-End-Transformation umzusetzen. Wir erweitern Ihren digitalen Fußabdruck und fördern nachhaltiges Unternehmenswachstum.

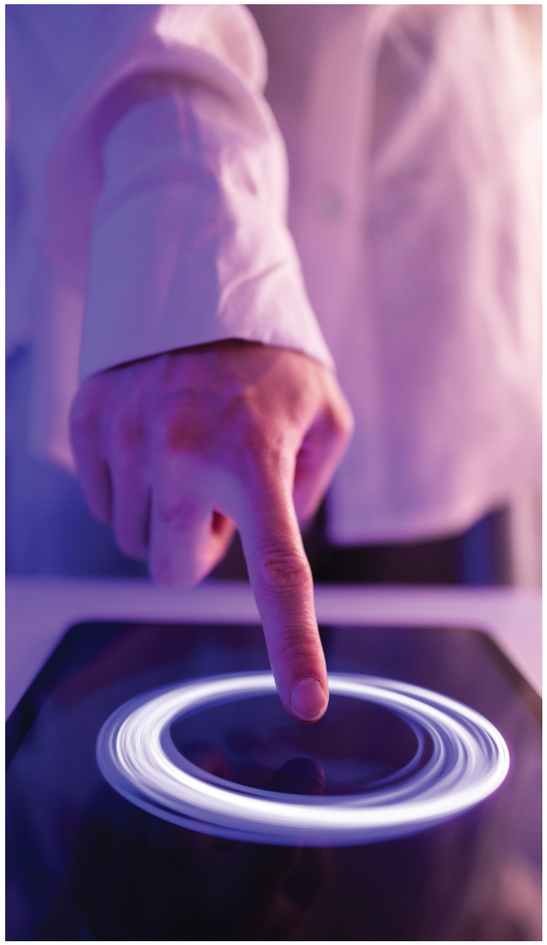
Intelligent Industry ist die nächste Generation der digitalen Transformation.
Neue disruptive Technologien und Daten sind allgegenwärtig und sorgen für radikale Veränderungen in allen Industriezweigen. Branchenführende müssen auf die daraus resultierende Transformationswelle reagieren, die den Wettbewerb stark beeinflusst und die Grenzen der Branche neu definieren wird. Als langfristiger Partner von Industrieunternehmen aller Branchen verändern wir in großem Umfang die Welt der Technik, der Lieferketten, der Fertigung und des Service. Wir entwickeln intelligente Produkte, Abläufe und Dienstleistungen und lösen geschäftliche, menschliche und technologische Herausforderungen.

Wir verbessern die betriebliche Leistung und schaffen neue Einnahmequellen in einer cybersicheren Welt, indem wir den Menschen, den Planeten und die Daten in den Mittelpunkt unseres Handelns stellen. Wir nutzen unsere Marken Cambridge Consultants und Synapse, um bahnbrechende Innovationen zu entwickeln, die unseren Kunden Wettbewerbsvorteile verschaffen.

Mehr Daten heißt auch mehr Datenschutz.
Als globale Unternehmensberatung lösen wir auch internationale datenschutzrechtliche Herausforderungen unserer Kunden. Dabei beobachten wir, dass – nachdem in den letzten Jahren vorallem die DSGVO im Fokus stand – mittlerweile die Aufmerksamkeit stärker auf Datenschutzrichtlinien außerhalb der EU gerichtet wird. Da die Komplexität in anderen Rechtsräumen mitunter deutlich höher ist als die bekannten DSGVO-Anforderungen, herrscht hier noch große Unsicherheit.

Wir haben bereits erfolgreich unsere Kunden bei der Analyse von über 45 Datenschutzgesetzen in Nicht-DSGVO-Ländern unterstützt und bringen Erfahrung bei der Definition von Target Operating Models für Datenschutzorganisationen mit. Gemeinsam mit unseren Kunden verfolgen wir einen pragmatischen Ansatz, in dem wir bestehende aus der DSGVO hervorgegangene Organisationsstrukturen, Prozesslandschaften und Technologien für die Erfüllung von Nicht-DSGVO-Richtlinien nutzbar machen. Dabei bieten wir als Capgemini-Gruppe auch unsere End-to-End-Services an und unterstützen Sie dabei, Rechts-, IT- und Fachbereiche aufeinander abzustimmen und Lösungen technisch umzusetzen, sodass Sie Ihre Datenschutzziele erreichen können.

Unsere Teams können auch Ihre Datenschutzorganisation auf die Anforderungen von Nicht-EU-Ländern vorbereiten.



Methodisches Vorgehen

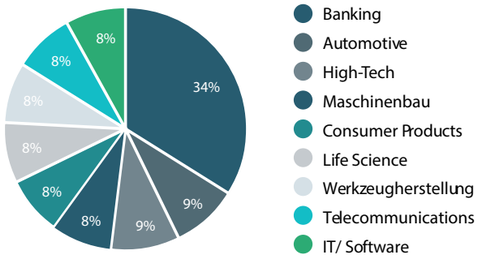
Welche Unternehmen uns Rede und Antwort standen

Im Rahmen unserer Studie wurde eine quantitative Umfrage mit über 100 ausgewählten Unternehmen in Deutschland hinsichtlich ihrer Selbsteinschätzung des Verständnisses und der Umsetzung weltweiter datenschutzrechtlicher Maßnahmen durchgeführt. Diese Unternehmen wurden anhand der Kriterien eines Hauptsitzes innerhalb Deutschlands und vorhandener internationaler Geschäftstätigkeit ausgewählt. An der finalen Studie haben ein Sechstel der befragten Unternehmen teilgenommen.

Von diesen sind 34% in der Bankingbranche tätig, die restlichen 66% teilen sich in 8 weitere Branchen auf, welche der Grafik 11 zu entnehmen sind. 59% der Befragten gehören der Abteilung des Data Protection Officers an, 25% dem Legal Bereich und jeweils 8% sind in der IT oder im Marketing / Sales aktiv. Der Jahresumsatz lag bei 8% der Unternehmen unter €500 Mio., bei der Mehrheit (58%) zwischen €500 Mio. & €5 Mrd. und bei jeweils 17% der Befragten lag der letzte Jahresumsatz bei entweder €10 Mrd. - €100 Mrd. oder bei mehr als €100 Mrd.

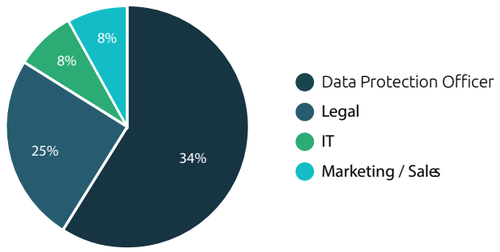
Zur Durchführung der Umfrage wurde ein Online-Fragebogen verwendet. Bei der Auswahl der teilnehmenden Personen wurde explizit darauf geachtet, dass diese innerhalb ihrer Organisation Entscheidungsträger mit einem fortgeschrittenen Datenschutzwissen sind. Der Fragebogen wurde in sechs Abschnitte gegliedert und enthielt 35 Fragen von allgemeiner Natur über die teilnehmenden Unternehmen bis hin zum Verständnis und zur Umsetzung einer Datenschutzkultur und Compliance mit Hinblick auf DSGVO und Nicht-DSGVO Regulierungen im jeweiligen Unternehmen. Des Weiteren wurden auch die Herausforderungen, welche datenschutzgetriebene Themen mit Hinblick auf Nicht-DSGVO Regulierungen mit sich bringen, betrachtet.

In welchen Industrien sind befragte Unternehmen tätig?



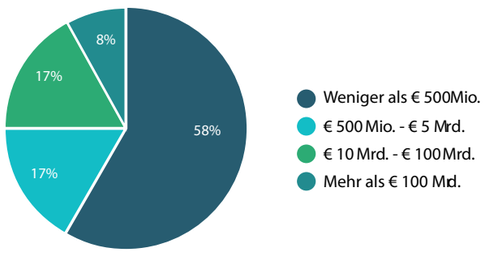
INDUSTRIEN

Welchen Abteilungen gehören befragte Datenschutzexpert*innen an?



ABTEILUNGEN

Wie hoch ist der Jahresumsatz befragter Unternehmen?



JAHRESUMSATZ

Über die Autoren

Marian Meyer-Tischler
Senior Director
Enterprise Data and Analytics | Capgemini Invent
marian.meyer-tischler@capgemini.com

Marian berät und begleitet unsere Kunden mit seinen branchenübergreifenden regulatorischen und Datenmanagementkenntnissen. Zusammen mit seinem Team spezialisiert er sich auf datenschutzrechtliche Herausforderungen, die mit dem wachsenden Angebot von digitalen Produkten und Services immer komplexer werden.

Jan Windheuser
Senior Manager
Enterprise Data and Analytics | Capgemini Invent
jan.windheuser@capgemini.com

Jan unterstützt unsere Kunden vor allem bei Themen rund um Datenschutz und Informationssicherheit. Dabei blickt er auf mehr als 20 Jahre Erfahrung in der IT-Industrie zurück, welche er in den verschiedensten Branchen gesammelt hat. Sein Fokus liegt dabei auf Projekten zur digitalen Transformation, vornehmlich in den Bereichen Automotive und Public Sector.

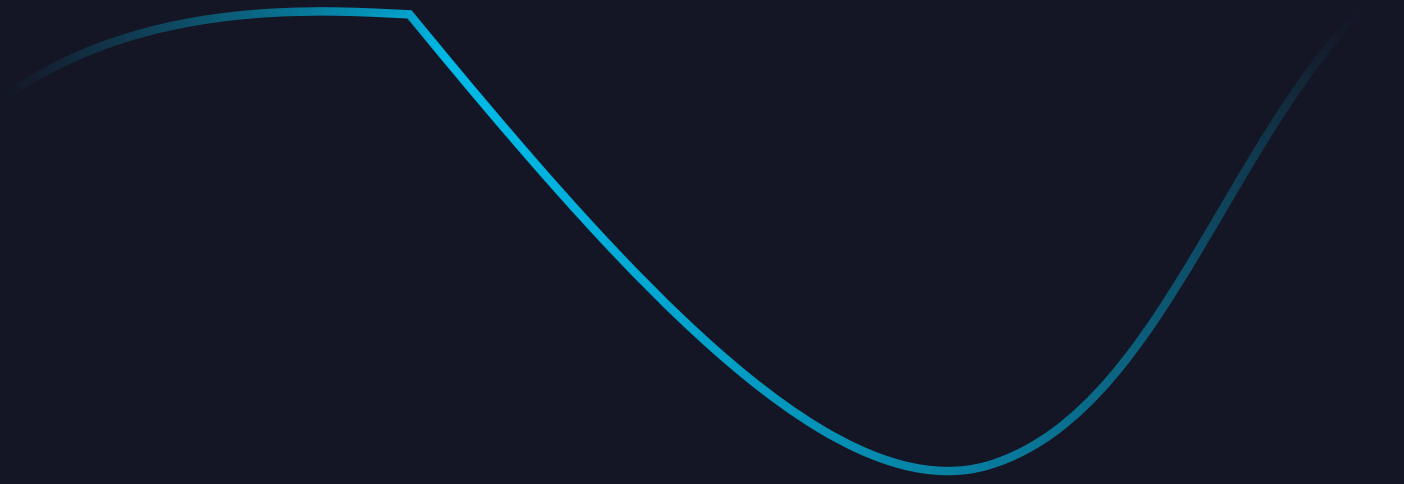
Kristina Heizenreder
Manager
Enterprise Data and Analytics | Capgemini Invent
kristina.heizenreder@capgemini.com

Kristina beschäftigt sich vornehmlich mit dem internationalen Datentransfer und seinen ständig wechselnden Herausforderungen durch Urteile oder neue Gesetzgebungen. Aufgrund ihrer Erfahrung bei der Durchführung von internationalen Datenschutz-Audits und in der Prozessberatung bietet sie ihren Kunden eine effiziente Lösung im Rahmen der datenschutzrechtlichen Möglichkeiten an.

Fabian Sünkler
Manager
Business Technology | Capgemini Invent
fabian.suenkler@capgemini.com

Fabian unterstützt unsere Kunden bei der Konzeption von skalierbaren Datenschutzorganisationen. Sein Fokus liegt insbesondere auf der Automobilindustrie, welche mittlerweile mit „Connected Vehicle-Data" Unmengen an Daten generiert und dessen Fahrzeughersteller zu grenzübergreifenden Datenverarbeitern geworden sind. Die steigende Komplexität verlangt daher nach modularen Lösungen.

Ein besonderer Dank für Ihren Beitrag an dieser Studie geht an Johan Rüggeberg, Katrin Frohoff-Hülsmann und Natalie Kerres.



About
Capgemini Invent

As the digital innovation, design and transformation brand of the Capgemini Group, Capgemini Invent enables CxOs to envision and shape the future of their businesses. Located in more than 36 offices and 37 creative studios around the world, it comprises a 12,000+ strong team of strategists, data scientists, product and experience designers, brand experts and technologists who develop new digital services, products, experiences and business models for sustainable growth.

Capgemini Invent is an integral part of Capgemini, a global leader in partnering with companies to transform and manage their business by harnessing the power of technology. The Group is guided everyday by its purpose of unleashing human energy through technology for an inclusive and sustainable future. It is a responsible and diverse organization of over 350,000 team members in more than 50 countries. With its strong 55-year heritage and deep industry expertise, Capgemini is trusted by its clients to address the entire breadth of their business needs, from strategy and design to operations, fueled by the fast evolving and innovative world of cloud, data, AI, connectivity, software, digital engineering and platforms. The Group reported in 2023 global revenues of €22.5 billion.

Get the Future You Want | www.capgemini.com/invent

Capgemini invent