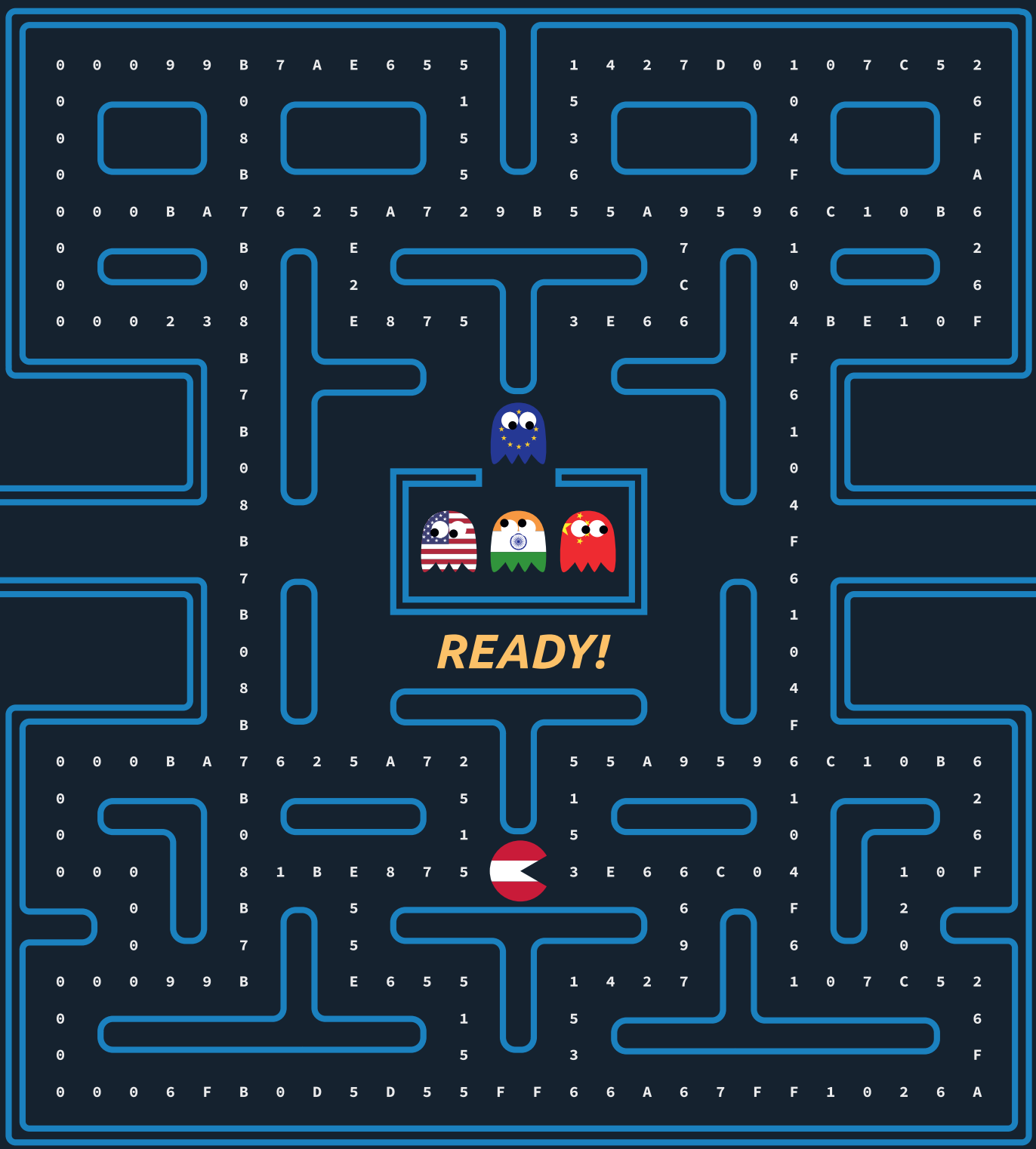
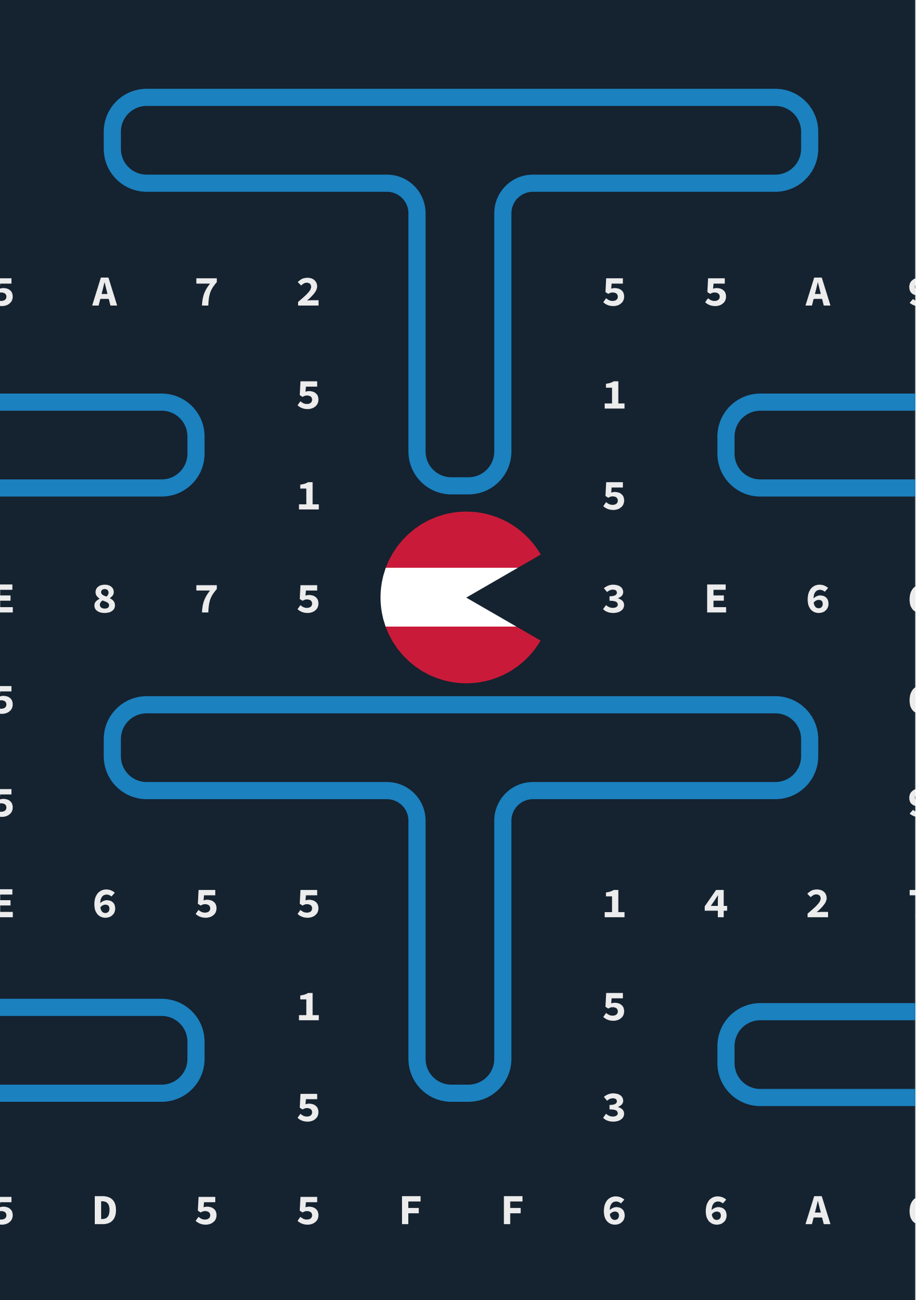
Capgemini invent



Wenn die DSGVO an ihre Grenzen stößt

Österreichische Unternehmen und ihr Umgang mit Datenschutzgesetzen aus Drittstaaten


5 A 7 2 5 5 A
5 1
1 5
E 8 7 5 3 E 6
5
5
E 6 5 5 1 4 2
1 5
5 3
5 D 5 5 F F 6 6 A

Vorwort

Seit dem 25. Mai 2018 hat sich viel verändert: Datenschutzgesetze sind weltweit auf dem Vormarsch. Ihre Durchsetzung nimmt zu und ist oftmals „exterritorial". So gelten nationale Vorschriften von „Drittstaaten" auch für österreichische Unternehmen, wenn diese personenbezogene Daten von Bürger*innen in Drittstatten oder innerhalb des jeweiligen Landes verarbeiten. In einer globalisierten Welt, in der insbesondere digitale Produkte und Dienstleistungen überall konsumiert werden können, summieren sich ausländische Datenschutzbestimmungen und fordern so die heute nur DSGVO-regulierten Datenschutzorganisationen österreichischer Unternehmen heraus.

Diese Studie soll herausfinden, wie österreichische Unternehmen mit DSGVO- und Nicht-DSGVO-Richtlinien in Hinblick auf Datenschutzkultur und Datenschutz-Compliance umgehen. Dabei befasst sich die Studie mit folgenden Fragen:

- Wie gut sind heimische Unternehmen auf Datenschutzgesetze von Drittstaaten vorbereitet?
- Welche Datenschutzherausforderungen sind dabei die größten?
- Was benötigen global tätige österreichische Unternehmen für ihre Zukunft?

Um Antworten auf diese Fragen zu finden, wurde das Thema mit Datenschutzverantwortlichen österreichischer Unternehmen aus unterschiedlichen Industrien in einer quantitativen Umfrage beleuchtet. Zudem wurden qualitative Fokusinterviews durchgeführt um einen Einblick in den Umgang mit Datenschutz und Datenschutzanforderungen aus Nicht-EU-Ländern zu erhalten. Ein besonderes Augenmerk wurde dabei auf das unternehmensspezifische Wissen im Zusammenhang mit Fragestellungen von Nicht-DSGVO-Richtlinien gelegt. Der seit der Einführung der DSGVO weltweit erkennbare Trend zeigt, dass die Regulierung personenbezogener Daten zunehmen wird. Daher ist es für jedes international tätige Unternehmen empfehlenswert sich bereits frühzeitig mit der weltweiten Regulierung personenbezogener Daten zu befassen. Klar ist: Zukünftig werden immer mehr personenbezogene Daten verarbeitet. Jetzt den Anschluss an eine globale Datenschutzentwicklung zu verlieren und sich aufgrund der DSGVO-Compliance in Sicherheit zu wägen ist riskant. Viele regulatorische Anforderungen unterscheiden sich nicht in ihrer Essenz, sondern im Detail. Aber im Detail steckt bekanntlich der Teufel. Umso wichtiger ist es für österreichische Unternehmen sich mit diesen regulatorischen Details auseinanderzusetzen und bestehende Datenschutzprozesse entsprechend zu skalieren.

Wir sind der festen Überzeugung, dass Datenschutz nachhaltig gestaltet werden muss, um die Zukunftsfähigkeit der eigenen Datenschutzorganisation sicherzustellen. Mit dieser Studie möchten wir dazu beitragen die Vielzahl internationaler Datenschutzentwicklungen sichtbar zu machen und damit einhergehende Handlungsfelder für österreichische Unternehmen aufzuzeigen.

Inhalt

DSGVO als Trendsetter

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

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.

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.

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.

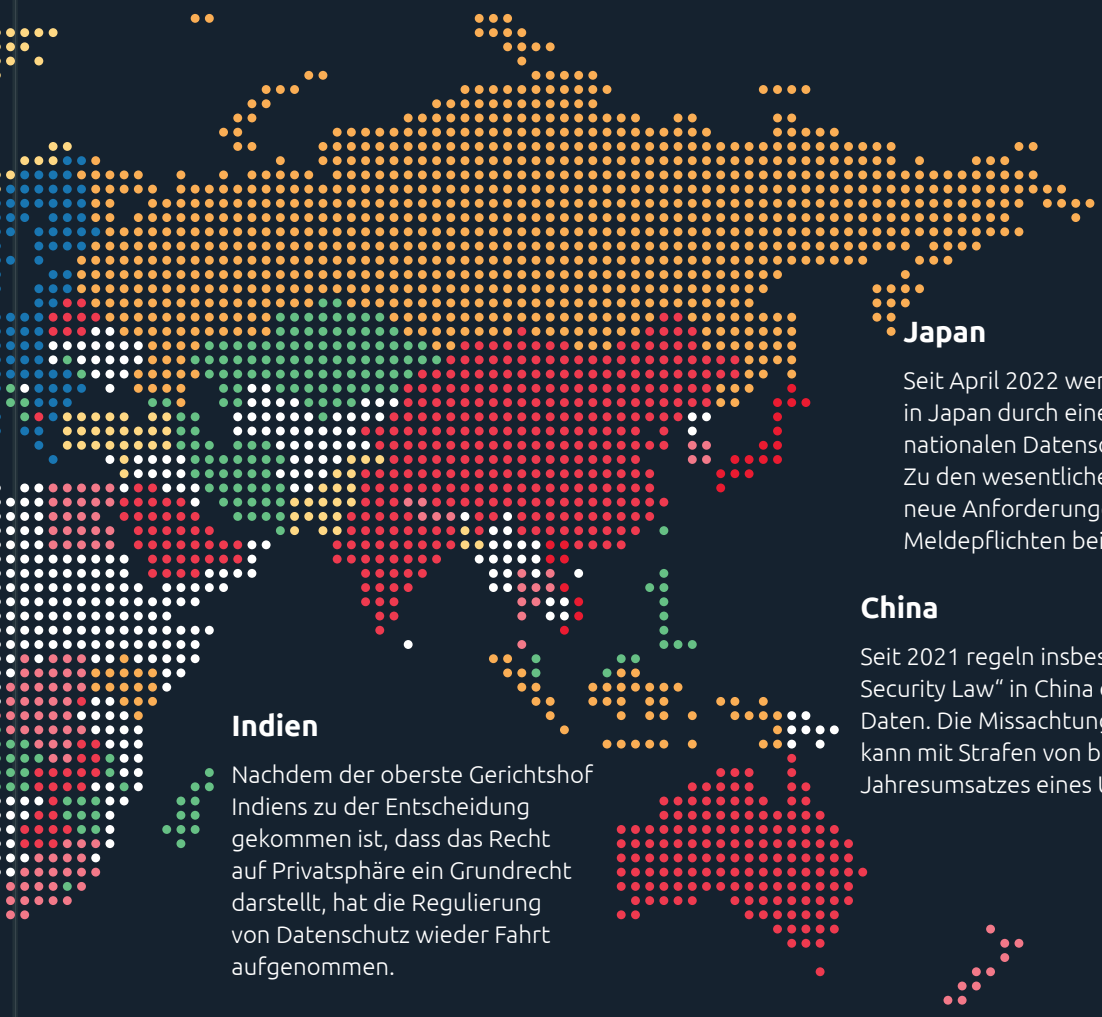
Argentinien

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.

F B 0 D 9 5 D 5 5 F F 6 R



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.

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.

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.

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.

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.

R I 9 3 H J 2 J N 5 5 0 0 4 F U

Österreichische Unternehmen kennen sich tendenziell schlecht mit Datenschutzgesetzen in Drittstaaten aus

Österreichische Unternehmen und internationaler Datenschutz

Mit einer Exportquote von über 50% profitiert die österreichische Wirtschaft stark vom internationalen Handel. Trends zeigen, dass der Anteil an Exporten zukünftig weiter steigen und im Jahr 2023 auf 56,8% heranwachsen wird. Dabei stehen nicht nur EU-Länder im Fokus. Vergleicht man den Zuwachs an Exporten zwischen EU- und Nicht-EU-Ländern, so ist festzustellen, dass die Zuwachsrate seit dem Jahr 2000 fast doppelt so hoch in Nicht-EU-Länder ist wie in EU-Ländern. Heute exportiert die österreichische Wirtschaft rund 30% in Nicht-EU-Länder, allen voran Asien, Amerika und restliche europäische Nicht-EU-Länder. (WKO, 2022)

Bei ihrem Export in mehr als 200 Länder, sehen sich österreichische Unternehmen mit vielen verschiedenen Datenschutzrichtlinien konfrontiert. Anzunehmen, dass eine DSGVO-Compliance auch alle Anforderungen von Drittstaaten erfüllt, ist falsch. Lokale Datenschutzrichtlinien unterscheiden sich nicht nur in ihrer Auslegung, sondern auch in der Art und Weise wie lokale Datenschutzbehörden diese durchsetzen und welche Anforderungen sie an ausländische Unternehmen stellen. Auch wenn die EU mit der DSGVO Vorreiter in Sachen Datenschutz ist, sehen wir, dass immer mehr Nicht-EU-Länder eigene Datenschutzrichtlinien verfassen. Die Vielzahl an länderspezifischen Anforderungen stellen Datenschutzbeauftragte österreichischer Unternehmen vor enorme Herausforderungen.

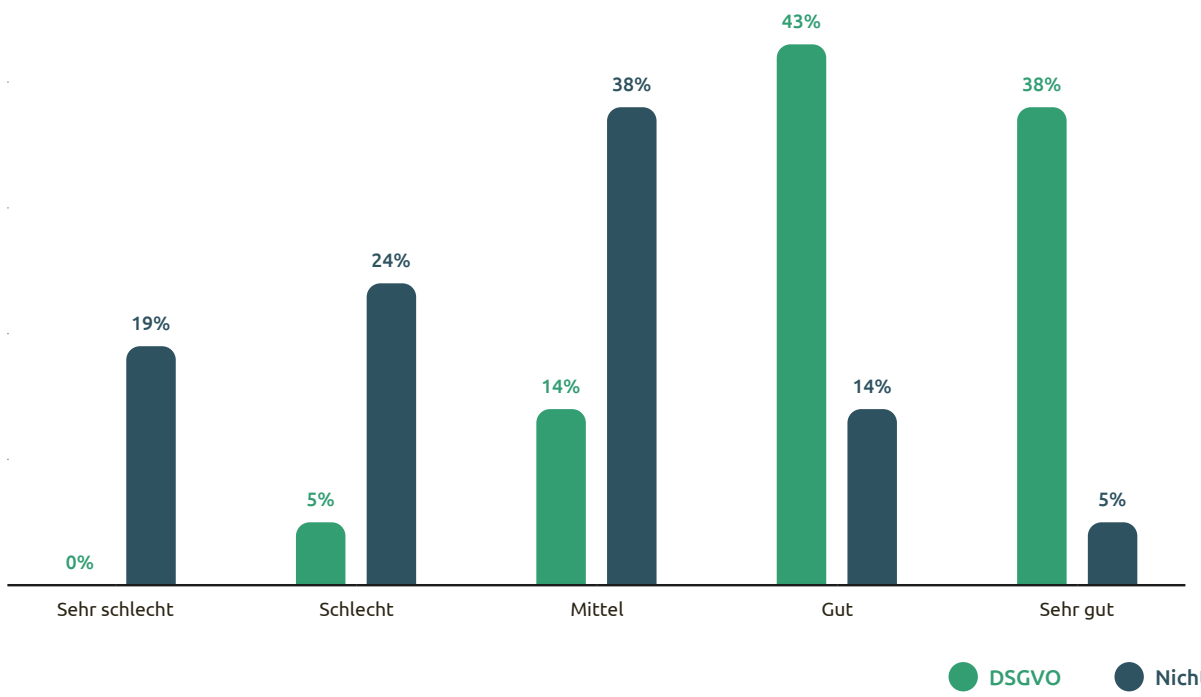
Wie Datenschutzverantwortliche österreichscher Unternehmen mit diesen Herausforderungen umgehen, haben wir in unserer Studie untersucht. Wenig überraschend, aber dennoch hervorzuheben ist, dass das Wissen über die DSGVO und die damit verbundenen Anforderungen deutlich höher ist als das Wissen über Datenschutzrichtlinien und dessen Einhaltung in Nicht-EU-Ländern. So gaben 43% der Befragten an über ein schlechtes oder sehr schlechtes Wissen im Hinblick auf Datenschutzrichtlinien in Drittstaaten zu verfügen. Lediglich 19% der Befragten schätzen ihr Wissen als gut oder sehr gut ein.

Wir sind in Europa und müssen uns schon lange mit der DSGVO auseinandersetzen. Selbst hier gibt es noch unklare Bereiche. Wenn man sich allein die USA anschaut, ist der Datenschutz schon sehr kompliziert. Das trifft auch zu, wenn man beispielsweise in Richtung China schaut.

Unternehmensjurist, Fahrzeugbau

0 D 9 5 D 5 5 F F 6 R

Diagramm 1: Wie schätzen die Befragten ihr Wissen bei der Beantwortung von Fragen zur Vorbereitung ihres Unternehmens auf die Einhaltung von DSGVO- und Nicht-DSGVO-Richtlinien ein?



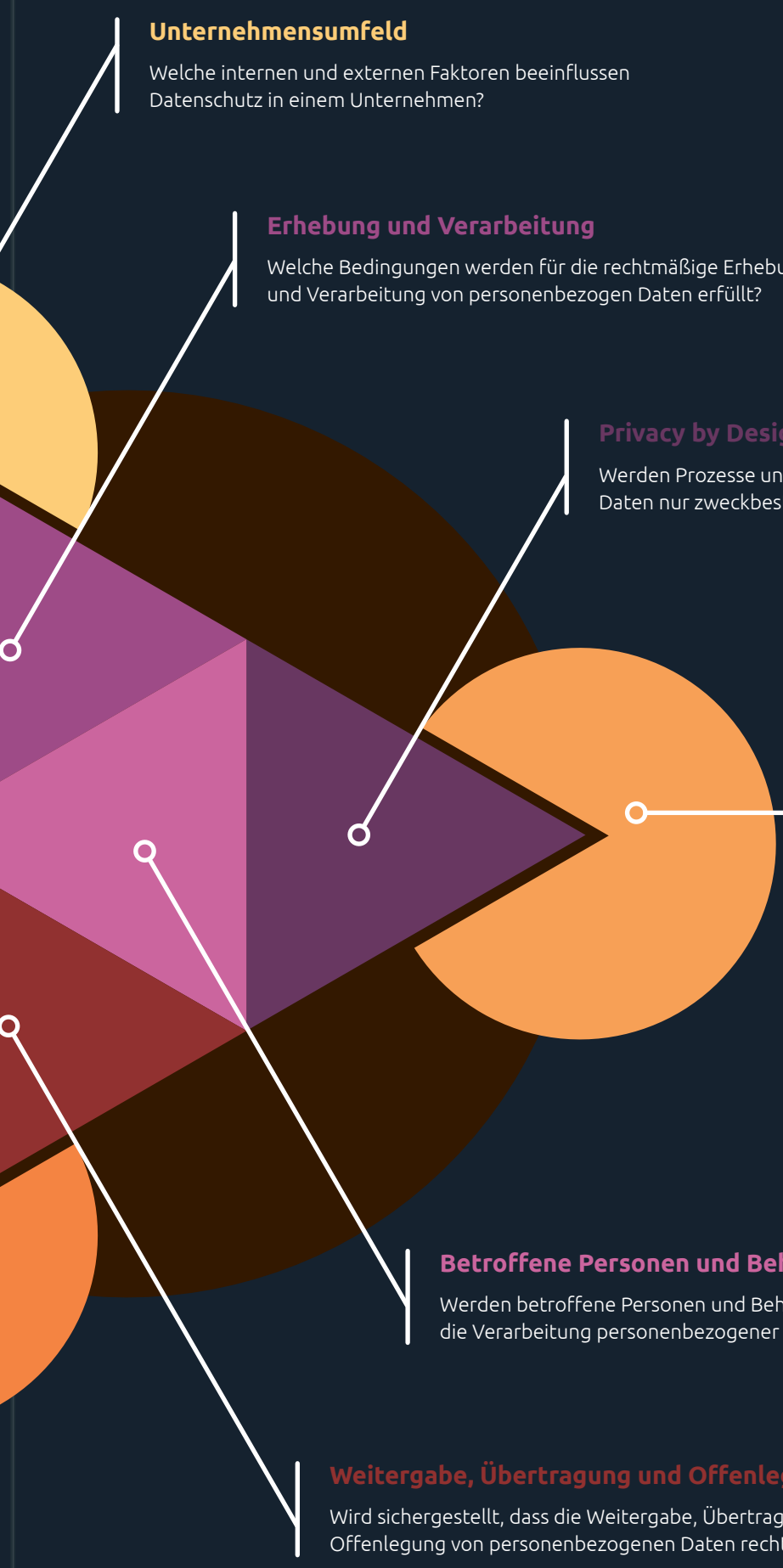
Nachhaltige Datenschutzorganisation

Datenschutz muss unternehmensweit gelebt werden

Wir durften bereits viele Unternehmen bei ihrer Transformation begleiten und konnten beobachten, wie die Einführung der DSGVO österreichische 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 österreichische Unternehmen befragt.



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?

R I 9 3 H J 2 J N 5 5 0 0 4 F U

Mehr als ⅔ der befragten Unternehmen unterschätzen die Relevanz von Datenschutzgesetzen 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 exterritorialen Anwendbarkeit konfrontiert. Diese externen Faktoren fallen in Abhängigkeit der Geschäftsmodelle und internationalen Ausrichtung österreichischer 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 rechtlicher Anforderungen in den jeweiligen Ländern. Neben den externen bestimmen auch interne Faktoren maßgeblich den Reifegrad der Datenschutzorganisation eines Unternehmens. Ganz unabhängig von der internationalen Ausrichtung eines Unternehmens, wirken sich unter anderem die individuellen Unternehmensrichtlinien und -verfahren auf den Umgang mit Datenschutzanforderungen aus.

Mit Blick auf Österreich, haben wir uns die Frage gestellt, wie österreichische Unternehmen mit den unterschiedlichen externen, wie auch internen Faktoren umgehen und welche Auswirkung das Unternehmensumfeld auf die Datenschutzorganisationen hat.

Österreichische Unternehmen messen externen und internen Faktoren einen unterschiedlichen Wert zur Erreichung ihrer Datenschutzziele bei. So schätzen die befragten Unternehmen interne Faktoren als relevanter für die Erreichung ihrer Nicht-DSGVO Datenschutzziele ein als die externen Faktoren. Auffällig ist, dass 95% der befragten Unternehmen die DSGVO als maßgeblichen externen Faktor für die Erreichung ihrer Datenschutzziele identifiziert haben. Gleichzeitig sind nur 29% der Unternehmen der Meinung, dass Nicht-DSGVO-Richtlinien relevant für ihre Datenschutzziele sind. Auch werden im Vergleich zur DSGVO, Vorschriften von Datenschutzbehörden und gerichtliche Entscheidungen in Nicht-DSGVO-Ländern als relevanter eingeschätzt als deren Datenschutzgesetze. Unter den internen Faktoren gaben 81% der Unternehmen im Kontext der DSGVO Unternehmensrichtlinien und -verfahren als relevanten Faktor zur Erreichung ihrer Datenschutzziele an. Im Kontext von Nicht-DSGVO-Ländern, halten 67% der Unternehmen Unternehmensrichtlinien und -verfahren für relevant. Ein ähnliches Bild zeichnet sich bei vertraglichen Anforderungen und Verwaltungsentscheidungen ab.

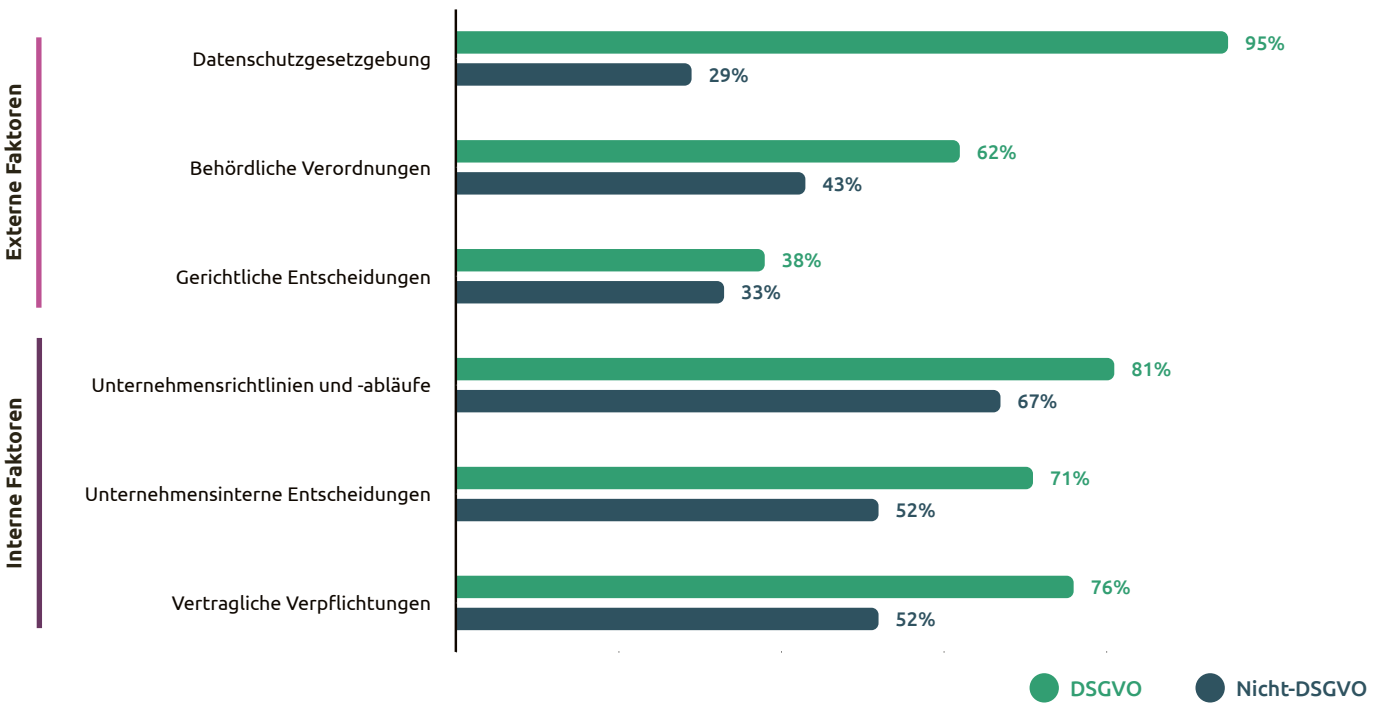
Zusammenfassend herrscht unter den befragten Unternehmen im Kontext der DSGVO eine größere Einigkeit darüber, welche Faktoren für die Datenschutzzielerreichung relevant sind als im Kontext von Nicht-DSGVO-Richtlinien.

Grundsätzlich steht und fällt alles mit der Schaffung interner Strukturen und der Betrachtung interner Faktoren!

Compliance Officer, Chemiebranche

D 5 5 F F 6 R

Diagramm 2: Wie viele der befragten Unternehmen halten folgende Faktoren in ihrem Unternehmensumfeld für relevant oder sehr relevant, um gesetzte Datenschutzziele zu erreichen?



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.

Aufsichtsbehörden werden als wenig relevant für die Verarbeitung personenbezogener Daten in Nicht-DSGVO-Ländern angesehen

Stakeholder Management

Um Datenschutzvorgaben in einem Unternehmen gesetzeskonform umsetzen zu können, wird der regelmäßige Austausch mit internen und externen Stakeholdern benötigt. 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 und 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 natürlich auch die Ansprechpartner*innen im eigenen Unternehmen über Datenschutzmaßnahmen informiert und für notwendige Aktivitäten mobilisiert werden. Beispielsweise sind auf der Seite der internen Stakeholder die Prozessverantwortlichen des jeweiligen Unternehmens für die Umsetzung von Datenschutzrichtlinien eine Schlüsselfigur, da sie etwaige Vorgaben in ihre Abläufe integrieren müssen.

Wir haben uns gefragt welche Relevanz die unterschiedlichen Stakeholder im Umgang mit personenbezogenen Daten aus Sicht österreichischer Unternehmen haben.

Für die Mehrheit der österreichischen Unternehmen sind die Ansprechpartner*innen im eigenen Unternehmen relevanter als externe Stakeholder. So ist auch erkennbar, dass die befragten Unternehmen Nicht-DSGVO-Richtlinien eine untergeordnete Rolle zuschreiben. Lediglich 24% der befragten Unternehmen erachten Nicht-DSGVO-Aufsichtsbehörden als relevante Ansprechpartner. Im Gegensatz dazu halten 57% der Unternehmen DSGVO-Aufsichtsbehörden für relevante Stakeholder.

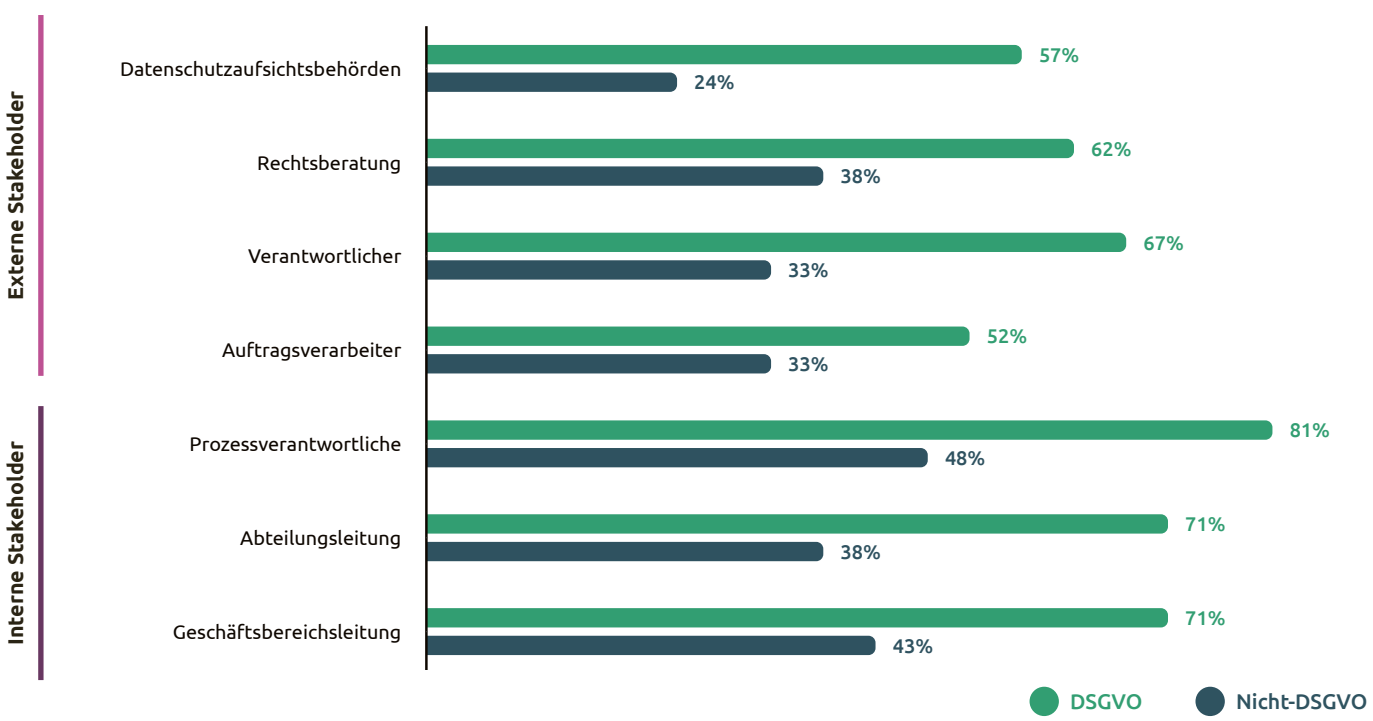
Lediglich 38% der befragten Unternehmen erachten Rechtsberatungen für eine relevante Unterstützung bei der Frage nach dem Umgang mit personenbezogenen Daten in Nicht-DSGVO-Ländern. Bei DSGVO-Fragestellungen verlassen sich 62% der Unternehmen auf Rechtsberatungen. Erstaunlich ist, dass nur jedes vierte Unternehmen Aufsichtsbehörden in Nicht-DSGVO-Ländern als relevante Stakeholder wahrnimmt. Fast jedes zweite Unternehmen erachtet die internen Prozessverantwortlichen als relevanten Ansprechpartner im Hinblick auf Nicht-DSGVO-Richtlinien. Dies deckt sich mit der Erkenntnis aus dem Unternehmensumfeld, welche aufgezeigt hat, dass interne Faktoren für die befragten Unternehmen einen höheren Stellenwert darstellen als beispielsweise Datenschutzgesetze aus Nicht-DSGVO-Ländern.

Kennen Sie bereits die „Cyberspace Administration of China (CAC)“, welche als der Super-Regulator des chinesischen Datenschutzrechts bezeichnet wird? Oder das chinesische „Ministerium für Industrie und Informationstechnik (MIIT)“, welches 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, welchem unter anderem die chinesische Polizei untersteht? All diese Institutionen haben in China beim Thema Datenschutz ein Wörtchen mitzureden und betreuen ein Geflecht diverser Datenschutz- und Informationssicherheitsgesetze.

Wir schalten die Aufsichtsbehörden nur ein, wenn wir dies tun müssen. Zum Beispiel, wenn eine Meldung über Datenschutzverletzungen erfolgen muss.

Unternehmensjurist, Fahrzeugbau

Diagramm 3: Wie viele der befragten Unternehmen erachten nachfolgende externe und interne Stakeholder bei der Verarbeitung personenbezogener Daten für wichtig oder sehr wichtig?



R I 9 3 H J 2 J N 5 5 0 0 4 F U

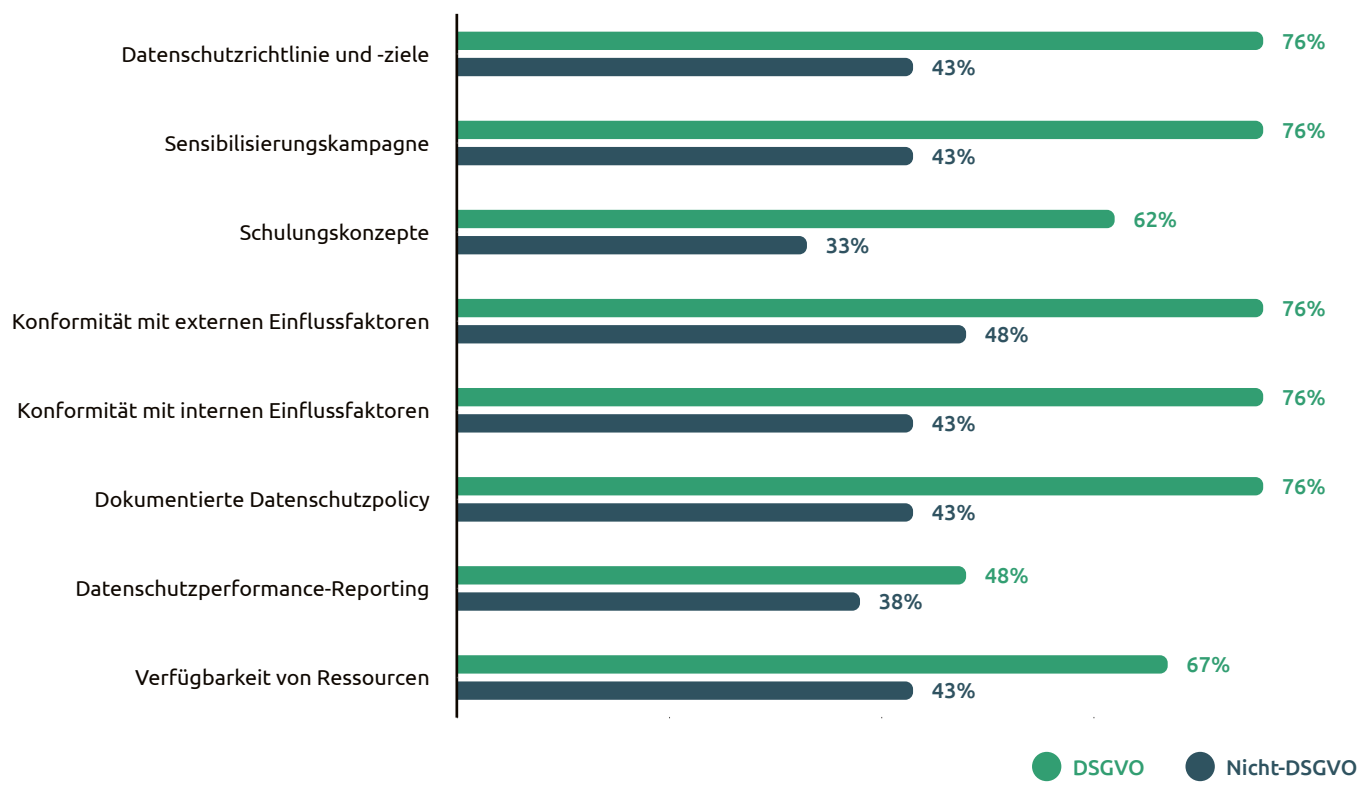
Nicht einmal jedes zweite befragte Unternehmen zeigt heute Leadership im Umgang mit Nicht-DSGVO-Vorschriften

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, steht 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 möchten wir uns einer Antwort annähern und haben gefragt, wie Führungskräfte österreichischer Unternehmen Führungsstärke in Bezug auf den Schutz personenbezogener Daten zeigen können.

Diagramm 4: Wie viele der befragten Unternehmen stimmen zu oder völlig zu, dass die Top-Managementebene Führungsstärke in Bezug auf den Schutz personenbezogener Daten in folgenden Punkten zeigt?



In Bezug auf die Art und Weise wie Führungsstärke bei datenschutzrelevanten Themen gezeigt werden kann, sind sich die befragten Unternehmen größtenteils einig. Unsere Studie ergab, dass vier von acht Antwortmöglichkeiten annähernd identisch bewertet wurden. Im Kontext der DSGVO nehmen 76% die Einhaltung externer Faktoren, interne Datenschutzrichtlinien und -ziele, Kommunikation, sowie die Einhaltung von unternehmensinternen Datenschutzrichtlinien als Zeichen für Führungsstärke in Bezug auf den Schutz personenbezogener Daten wahr. Ebendiese Antwortmöglichkeiten werden allerdings nur von rund 43% der befragten Unternehmen im Zusammenhang mit Nicht-DSGVO-Richtlinien angeführt.

Der Stellenwert von Datenschutz innerhalb eines Unternehmens zeichnet sich nicht nur durch den Umfang und die Kommunikation interner Datenschutzrichtlinien aus, sondern auch durch den für das Thema bereitgestellten Ressourcenumfang und dessen unabhängige organisatorische Einbindung in die entsprechenden Fachbereiche. Während im Kontext der DSGVO 67% der befragten Unternehmen verfügbare Ressourcen für relevant erachten, sehen nur 33% verfügbare Ressourcen als relevant für Nicht-DSGVO-Vorschriften an. Hier könnte ein geringer Reifegrad bestehender Prozesse, die damit verbundenen nicht definierten Rollen und Verantwortlichkeiten und das fehlende Bewusstsein für datenschutzrechtliche Anforderungen in Nicht-DSGVO-Ländern die Einschätzung begründen. Ein regelmäßiges Reporting des Datenschutzes halten 48% beziehungsweise 38% der Befragten für relevant.

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.

Wir haben verpflichtende Datenschutzschulungen, die wir weltweit durchführen und jährlich wiederholen. Auf dem Thema liegt hohe Attention seitens der Unternehmensführung.

Datenschutzbeauftragter, Informationstechnologieunternehmen

R I 9 3 H J 2 J N 5 5 0 0 4 F U

Jedes zweite befragte Unternehmen glaubt, dass ihre personenbezogenen Daten rechtmäßig in Drittstaaten verarbeitet werden

Erhebung und Verarbeitung

Eine Verarbeitungstätigkeit, welche personenbezogene Daten erhebt oder vorhandene Daten weiterverarbeitet, 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 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.

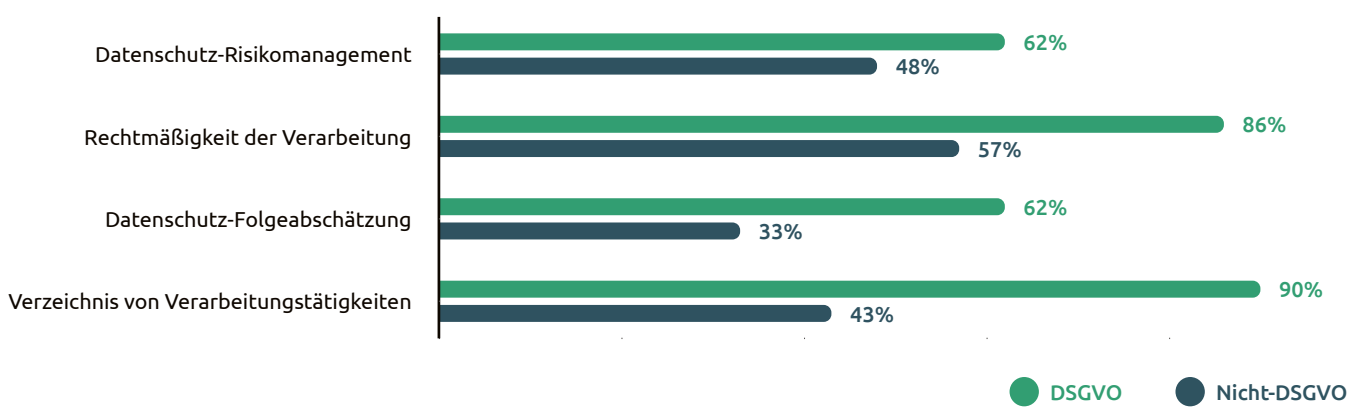
Unternehmen müssen daher sicherstellen und dokumentieren, dass auch die Verarbeitung von Daten aus Nicht-DSGVO-Ländern mit einer Rechtsgrundlage gemäß der geltenden Rechtsprechung und klar definierten und legitimen Zwecken erfolgt. Insbesondere Betroffene sollten den Zweck, zu dem ihre personenbezogenen Daten verarbeitet werden, verstehen. Ohne eine klare Information über den Zweck der Verarbeitung kann schließlich auch keine angemessene Einwilligung durch eine betroffene Person erfolgen. So sind auch Einwilligungserklärungen ein Aspekt, welcher 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 österreichische Unternehmen ihren eigenen Reifegrad im Hinblick auf die Erhebung und Verarbeitung personenbezogener Daten einschätzen.

Wie erwartet, schätzen die befragten Unternehmen ihren Reifegrad im Hinblick auf die DSGVO am höchsten ein. Am besten schneidet dabei das Verzeichnis von Verarbeitungstätigkeiten ab, welches von 90% der Unternehmen als ausgeprägt bis stark ausgeprägt bewertet wird. Schlusslicht im Rahmen der DSGVO sind mit jeweils 62% das Datenschutz-Risikomanagement und die Datenschutz-Folgeabschätzung. Auch für Nicht-DSGVO-Länder stellt die Datenschutz-Folgeabschätzung mit 33% den geringsten Reifegrad der befragten Unternehmen dar. Interessanterweise geben 57% der befragten Unternehmen an, dass sie die Rechtmäßigkeit der Verarbeitung ihrer personenbezogenen Daten in Nicht-DSGVO-Ländern für ausgeprägt bis stark ausgeprägt halten. Dieser Umstand ist insofern bemerkenswert, da zuvor die Analyse des Unternehmensumfelds gezeigt hat, dass lediglich 29% der befragten Unternehmen Nicht-DSGVO-Datenschutzgesetze für relevant erachten.

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 ein Fernsehbeitrag über Datentransfers nach China berichtete. 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.

Diagramm 5: Wie viele der befragten Unternehmen bewerten folgende Prozesse als ausgeprägt oder sehr ausgeprägt?



Wenn wir eine Verarbeitungstätigkeit durchführen, unabhängig davon, ob es sich um ein EU-Land oder ein Nicht-EU-Land handelt, wenden wir immer unsere Standards an. Das bedeutet, dass die Verarbeitungstätigkeit denselben Prozess durchläuft wie eine lokale Verarbeitungstätigkeit.

Compliance Officer, Chemiebranche

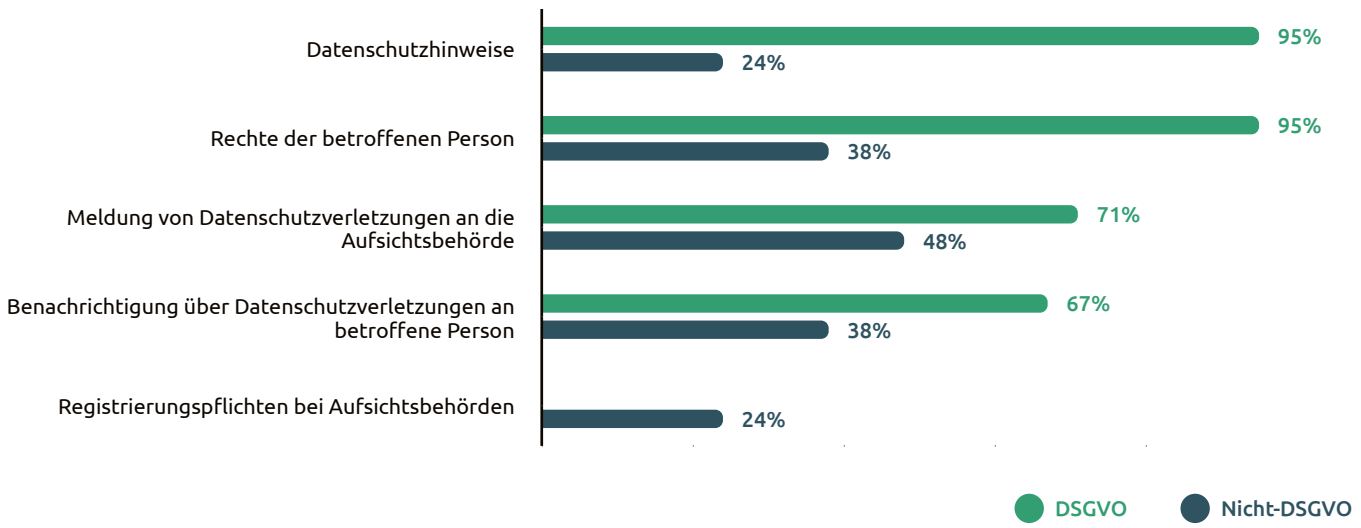
¾ der befragten Unternehmen glauben, dass ihre Datenschutzhinweise nicht den Vorgaben von Drittstaaten entsprechen

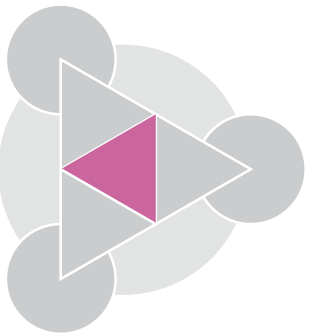
Betroffene Personen und Behörden

Unternehmen, die personenbezogene Daten verarbeiten, sind gemäß DSGVO und vielen Datenschutzgesetzen von 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 hohe Außenwirkung. Nicht umgesetzte oder nicht korrekt umgesetzte Informationspflichten stellen einen Datenschutzverstoß dar und können neben Bußgeldern auch erhebliche Reputationsschäden nach sich ziehen. Neben den Betroffenen selbst, sind Unternehmen auch gegenüber den jeweiligen Aufsichtsbehörden 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. In den USA müssen Unternehmen sogar die Anzahl an zurückgewiesenen Betroffenenrechteanfragen und die durchschnittliche Bearbeitungsdauer öffentlich machen.

Informationspflichten sind vielseitig und können bei Verstößen ernstzunehmende Konsequenzen nach sich ziehen. Gerade deshalb ist es für Unternehmen wichtig sich auch mit den rechtlichen Anforderungen in Nicht-EU-Ländern auseinander zu setzen. Daher haben wir uns die Frage gestellt, ob österreichische Unternehmen diesen Herausforderungen gewachsen sind.

Diagramm 6: Wie viele der befragten Unternehmen bewerten folgende Maßnahmen als ausgeprägt oder sehr ausgeprägt?





Auffällig ist, dass alle befragten Unternehmen die genannten Maßnahmen im Kontext der DSGVO für ausgeprägter halten als für Nicht-DSGVO-Richtlinien. Grund könnte hier die allgemeine Unsicherheit über die in Drittstaaten geltenden Informationspflichten sein. Darüber hinaus bestehen sicherlich auch Herausforderungen in der Umsetzung von verschiedenen Datenschutzanforderungen. Während beispielsweise 95% der befragten Unternehmen ihre Datenschutzhinweise als ausgeprägte Maßnahme für die Einhaltung von Informationspflichten innerhalb der DSGVO bewerten, sehen nur 52% selbige Maßnahme als ausgeprägt für Nicht-DSGVO-Richtlinien an.

Auch wenn für Nicht-EU-Länder Registrierungsanforderungen bei einer Aufsichtsbehörde gelten, bewerten nur 24% der teilnehmenden Unternehmen diese Maßnahme zur Sicherstellung von Informationspflichten als ausgeprägt. Insbesondere vor dem Hintergrund, dass die Erfüllung von Registrierungsanforderungen in direktem Zusammenhang zu einer regulierenden Behörde steht, ist diese Maßnahme bei den befragten Unternehmen überraschend niedrig ausgeprägt. Im Umkehrschluss, bedeutet dies, dass drei von vier Unternehmen diese Maßnahme als nicht ausgeprägt in ihrer Organisation wahrnehmen.

Wir machen keine Unterschiede bei der Art und Weise wie wir Informationspflichten in EU- und Nicht-EU-Ländern nachkommen.

Compliance Officer, Chemiebranche

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 kann heute Privacy by Design/ Default Prinzipien gemäß DSGVO erfüllen

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 statt reaktives Handeln ist notwendig, um Datenschutz 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.

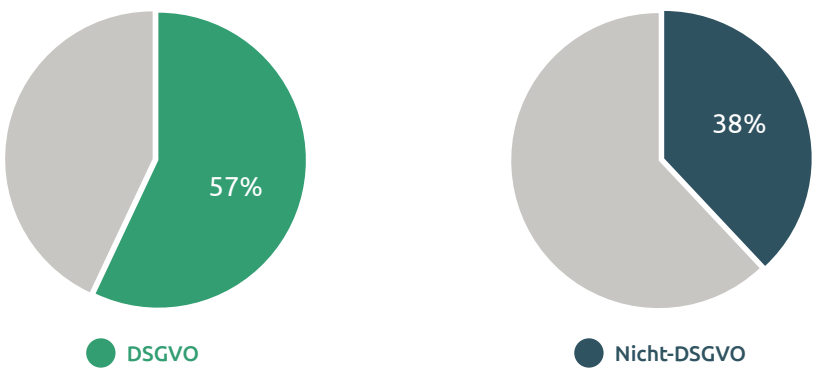
Diverse technische und organisatorische Maßnahmen können Privacy by Design/Default sicherstellen, weshalb es, Stand heute, keinen einheitlichen Ordnungsrahmen gibt. Da Maßnahmen stets entsprechend der durchzuführenden Verarbeitungstätigkeit und Rahmenbedingungen definiert werden, haben wir uns die Frage gestellt, wie österreichische Unternehmen dieser Herausforderung im heimischen und internationalen Markt begegnen.

Rund 57% der befragten österreichischen Unternehmen sind davon überzeugt, dass sie bereits heute Privacy by Design/ Default gemäß DSGVO sicherstellen. Mit Blick auf Nicht-DSGVO-Richtlinien sind nur 38% der befragten Unternehmen dieser Ansicht. An dieser Stelle wird erneut ersichtlich, dass technische und organisatorische Maßnahmen im Zusammenhang mit Nicht-EU-Ländern weniger ausgereift sind.

Gerade wenn es um Machine Learning oder Artificial Intelligence geht, gibt es immer viele Diskussionen, da der eigentliche Zweck der Verarbeitung meist noch nicht feststeht. Deswegen arbeiten wir viel mit Anonymisierung oder Pseudonymisierung!

Unternehmensjurist, Fahrzeugbau

Diagramm 7: Wie viele der befragten Unternehmen bewerten die technischen und organisatorischen Maßnahmen, die dafür sorgen, dass die Erhebung und Verarbeitung personenbezogener Daten auf das für den angegebenen Zweck erforderliche Maß beschränkt ist, als ausgeprägt oder sehr ausgeprägt?



Was passieren kann, wenn Privacy by Design/Default nicht nachhaltig umgesetzt wird, zeigt das Beispiel einer US-amerikanische 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 technisch-organisatorischen Maßnahmen nicht geeignet waren, um den Schutz der personenbezogenen Daten sicherzustellen. Daraus resultierte ein Bußgeld in Höhe von EUR 20 Millionen.

Trotz Wissenslücken, glaubt jedes zweite Unternehmen, dass grenzüberschreitende Datentransfers konform umgesetzt werden

Weitergabe, Übertragung und Offenlegung

Vor besonderen Herausforderungen stehen Unternehmen, 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 eben jener Daten macht.

Gemäß DSGVO dürfen personenbezogene Daten nur in jene Drittländer übermittelt werden, welche 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 österreichische Unternehmen für die Weitergabe, Übermittlung und Offenlegung von personenbezogenen Daten ergreifen und wie ausgeprägt diese in den jeweiligen Organisationen wahrgenommen werden.

76% der befragten Unternehmen geben an, dass die Anwendung von Auftragsverarbeitungsverträgen in ihrer Organisation einen hohen Reifegrad hat. Bei der Datenübermittlung in Nicht-DSGVO-Ländern sehen weniger als die Häfte der befragten Unternehmen eine hohe Ausprägung dieser Maßnahme. Bei der grenzüberschreitenden Datenübermittlung zeichnet sich sowohl für DSGVO als auch Nicht-DSGVO-Richtlinien ein ähnliches Bild ab. Hier bewerten in beiden Fällen rund die Hälfte der befragten Unternehmen, dass der Umgang mit grenzüberschreitenden Datenübermittlungen stark ausgeprägt ist. Datenlokalisierung/-residenz sehen nur 43% der teilnehmenden Unternehmen als ausgeprägt innerhalb ihrer Organisation an.

Die schwedische Datenschutzbehörde hat 2021 bei einem schwedischen Online-Zahlungsdienstleister festgestellt, dass das Unternehmen keine Auskunft darüber geben konnte in welche Länder außerhalb der EU/des EWR personenbezogene Daten übermittelt werden oder wo und wie Einzelpersonen Informationen, über die für die Übermittlung in Drittländer geltenden Garantien erhalten können. Damit hat das Unternehmen das Grundprinzip der Transparenz und das Recht der betroffenen Personen auf Information nicht erfüllt und wurde zu einer Geldstrafe von über EUR 700.000 verurteilt.

Diagramm 8: Wie viele der befragten Unternehmen bewerten folgende Maßnahmen hinsichtlich der Dokumentation der gemeinsamen Nutzung, Übermittlung und/oder Offenlegung personenbezogener Daten gegenüber anderen Rechtsordnungen oder Dritten, als ausgeprägt oder sehr ausgeprägt?

Wir haben sehr detaillierte Verträge mit unseren Stakeholdern in EU- und Nicht-EU-Ländern bezüglich der Nutzung und Übermittlung von personenbezogenen Daten. In diesen Verträgen wird festgelegt, wer die Daten besitzt, dafür verantwortlich ist und wer sie verarbeiten darf.

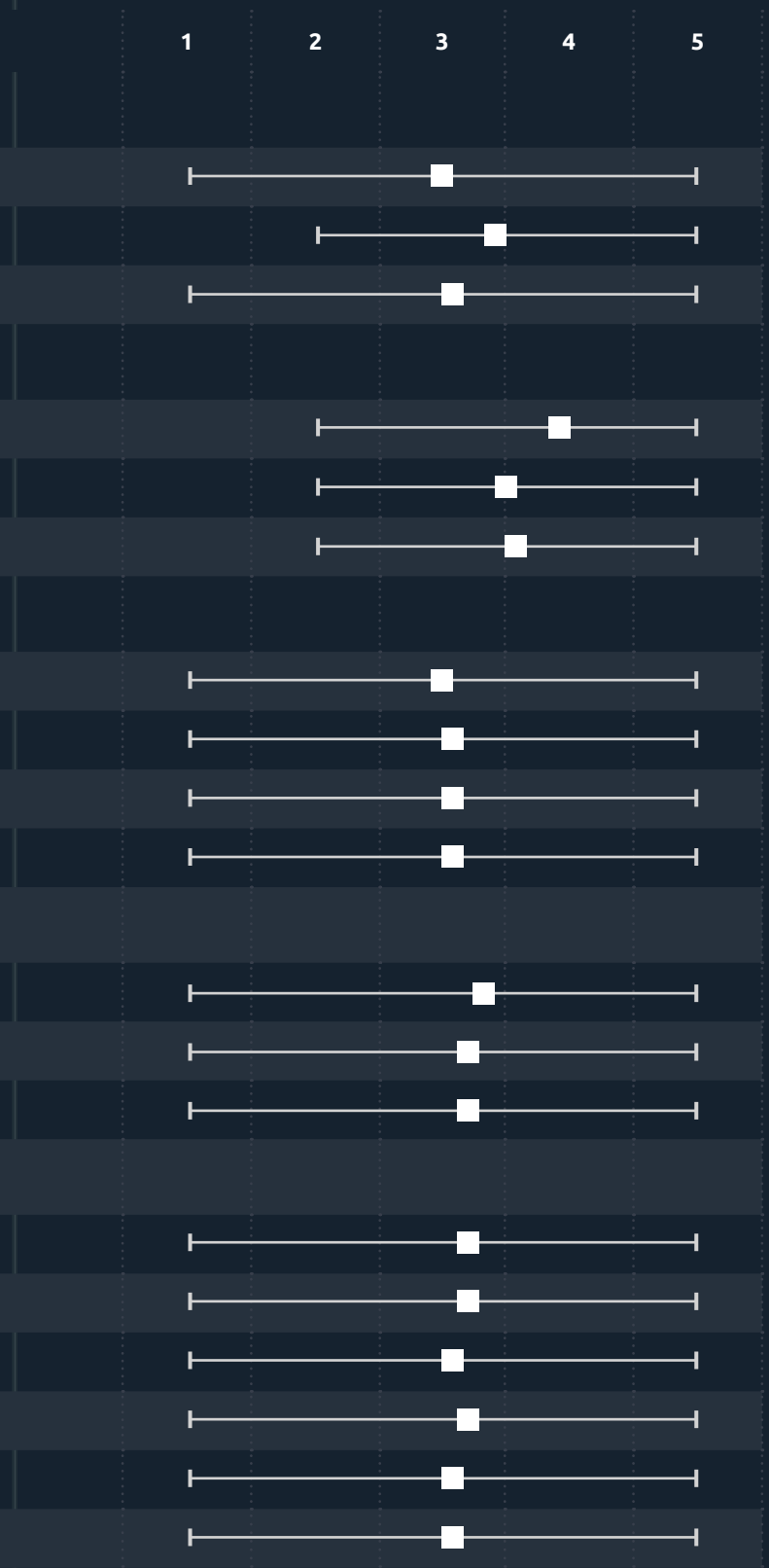
Compliance Officer, Industriebranche

Standortfeststellung

Wie gut sind Sie auf Datenschutzanforderungen aus Drittstaaten vorbereitet?

Datenschutzkultur

		1	2	3	4	5
Unternehmens-umfeld	**1. Wie relevant sind die nachfolgenden externen Einflussfaktoren für Ihr Unternehmen?**					
	a. Datenschutzgesetzgebung	☐	☐	☐	☐	☐
	b. Behördliche Verordnungen	☐	☐	☐	☐	☐
	c. Gerichtliche Entscheidungen	☐	☐	☐	☐	☐
	2. Wie relevant sind die nachfolgenden internen Einflussfaktoren für Ihr Unternehmen?					
	a. Unternehmensrichtlinien und -abläufe	☐	☐	☐	☐	☐
	b. Unternehmensinterne Entscheidungen	☐	☐	☐	☐	☐
	c. Vertragliche Verpflichtungen	☐	☐	☐	☐	☐
Stakeholder Management	**3. Wie relevant sind die nachfolgenden externen Stakeholder für Ihr Unternehmen?**					
	a. Datenschutzaufsichtsbehörden	☐	☐	☐	☐	☐
	b. Rechtsberatung	☐	☐	☐	☐	☐
	c. Verantwortlicher	☐	☐	☐	☐	☐
	d. Auftragsverarbeiter	☐	☐	☐	☐	☐
	4. Wie relevant sind die nachfolgenden internen Stakeholder für Ihr Unternehmen?					
	a. Prozessverantwortliche	☐	☐	☐	☐	☐
	b. Abteilungsleitung	☐	☐	☐	☐	☐
	c. Geschäftsbereichsleitung	☐	☐	☐	☐	☐
Leadership	**5. In welchen Bereichen zeigt das Top-Management Ihres Unternehmens Leadership und Einsatz?**					
	a. Datenschutzrichtlinie und -ziele	☐	☐	☐	☐	☐
	b. Sensibilisierungskampagne	☐	☐	☐	☐	☐
	c. Schulungskonzept	☐	☐	☐	☐	☐
	d. Konformität mit externen Einflussfaktoren	☐	☐	☐	☐	☐
	e. Konformität mit internen Einflussfaktoren	☐	☐	☐	☐	☐
	f. Datenschutzperformance-Reporting	☐	☐	☐	☐	☐



Unsere Studie zeigt auf, dass der Reifegrad entlang der beiden Dimensionen einer Datenschutzorganisation von der Internationalität eines Unternehmens abhängt. Die Tendenz zeigt, dass Unternehmen, die in mehreren Nicht-EU-Ländern aktiv sind, einen höheren Reifegrad für die Abdeckung internationaler Datenschutzanforderungen aufweisen als Unternehmen, die in wenigen Ländern außerhalb der EU geschäftlich aktiv sind.

Um den Reifegrad Ihres Unternehmens im Hinblick auf internationale Datenschutzanforderungen bestimmen und mit den befragten österreichischen Unternehmen aus unserer Studie vergleichen zu können, finden Sie auf der linken Seite die Kernfragen der beiden Dimensionen Datenschutzkultur und Datenschutz-Compliance. Mit diesem Self-Assessment können Sie eine grobe Standortfeststellung vornehmen und sich so auch mit den teilnehmenden Unternehmen unserer Studie vergleichen. Neben dem durchschnittlich angegebenen Reifegrad können Sie auch die höchste bzw. niedrigste Einwertung der befragten Unternehmen einsehen.

Bitte beantworten Sie die Fragen auf einer Skala von 1 (wenig zutreffend) bis 5 (stark zutreffend).

Datenschutz-Compliance

		1	2	3	4	5
Erhebung und Verarbeitung	**1. Wie schätzen Sie den Reifegrad für Ihr Unternehmen ein?**					
	a. Datenschutz-Risikomanagement	☐	☐	☐	☐	☐
	b. Datenschutz-Folgeabschätzung	☐	☐	☐	☐	☐
	c. Rechtmäßigkeit der Verarbeitung	☐	☐	☐	☐	☐
	d. Verzeichnis von Verarbeitungstätigkeiten	☐	☐	☐	☐	☐
Betroffene Personen und Behörden	**2. Wie schätzen Sie den Reifegrad für Ihr Unternehmen ein?**					
	a. Datenschutzhinweise	☐	☐	☐	☐	☐
	b. Rechte der betroffenen Person	☐	☐	☐	☐	☐
	c. Meldung von Datenschutzverletzungen an die Aufsichtsbehörde	☐	☐	☐	☐	☐
	d. Benachrichtigung über Datenschutzverletzungen an betroffene Person	☐	☐	☐	☐	☐
	e. Registrierungspflichten bei Aufsichtsbehörden	☐	☐	☐	☐	☐
Privacy by Design/Default	**3. Wie schätzen Sie den Reifegrad für Ihr Unternehmen ein?**					
	a. Privacy by Design/Default	☐	☐	☐	☐	☐
Weitergabe, Übertragung und Offenlegung	**4. Wie schätzen Sie den Reifegrad für Ihr Unternehmen ein?**					
	a. Auftragsverarbeitungsverträge	☐	☐	☐	☐	☐
	b. Grenzüberschreitende Datenübermittlung	☐	☐	☐	☐	☐
	c. Datenlokalisierung/-residenz	☐	☐	☐	☐	☐


1
2
3
4
5

Nur jedes vierte Unternehmen kennt Datenschutzanforderungen aus Drittstaaten

Herausforderungen aus Unternehmenssicht

Im Verlauf dieser Studie hat sich in allen betrachteten Dimensionen der Reifegrad von Unternehmen für die Erfüllung von DSGVO-Anforderungen als höher herausgestellt als bei Nicht-DSGVO-Richtlinien. Doch trotz dieses Ungleichgewichts zwischen DSGVO und Nicht-DSGVO-Ländern scheinen die Datenschutzgesetze von Drittstaaten nicht auf großes Interesse heimischer Unternehmen zu stoßen. Dabei stellen diese bei Missachtung ein hohes Risiko für die internationale Geschäftstätigkeit von österreichischen Unternehmen dar. Unsere Befragung zum Unternehmensumfeld hat gezeigt, dass lediglich für 29% der befragten Unternehmen Nicht-DSGVO Datenschutzgesetze relevant für ihre Datenschutzziele sind. Mangels dieser Relevanz besteht wohl auch mit 38% ein weitaus geringeres Interesse an externer Rechtsberatung zu Nicht-DSGVO Datenschutzgesetzen als es beispielsweise bei der DSGVO mit 68% der Fall ist. So zeigt auch unsere Untersuchung des Themenfeldes Stakeholder Management, dass die befragten Unternehmen bei Nicht-DSGVO Datenschutzgesetzen eher interne Ansprechpartner für relevant halten als beispielsweise Datenschutzbehörden in Nicht-DSGVO-Ländern. Was also passiert, wenn Unternehmen sich eher an der heimischen Gesetzgebung orientieren und nicht so recht über den europäischen Tellerrand hinausschauen möchten? Aus eben diesem Grund haben wir die an der Studie teilnehmenden Unternehmen nach ihren größten Herausforderungen im Hinblick auf Nicht-DSGVO Datenschutzgesetze gefragt.

Dabei hat sich herausgestellt, dass bei allen befragten Unternehmen Einigkeit darüber herrscht, dass das fehlende Verständnis über zu ergreifende Maßnahmen ihre größte Herausforderung darstellt. Die Unwissenheit über Nicht-DSGVO-Richtlinien beschäftigt 86% der Unternehmen beim Aufbau einer internationalen Datenschutz-Compliance. Fehlendes Wissen über neue Nicht-DSGVO-Richtlinien und notwendige Aktivitäten stellen jedoch nicht die einzige Herausforderung dar. So beschreiben drei von vier der befragten Unternehmen, dass der Umgang mit der Vielfalt unterschiedlicher Anforderungen eine Herausforderung für sie darstellt. Für rund die Hälfte der befragten Unternehmen ist das Schließen von Lücken in ihrer heutigen DSGVO-Compliance und die Erweiterung bestehender Datenschutzorganisationen eine Herausforderung auf dem Weg in Richtung internationale Datenschutz-Compliance.

Diagramm 10: Was sind die fünf größten Herausforderungen, wenn es um die Einhaltung von Nicht-DSGVO-Vorschriften geht?

Warum wir von nachhaltigem Datenschutz überzeugt sind

Unser Fazit

Die zunehmende Regulierung von Datenschutz sorgt weltweit einerseits für eine höhere Belastung der Compliancebereiche in Unternehmen und andererseits sind Datenschutz und Privatsphäre schon längst zu einem Bestandteil des eigenen Brandings geworden. Es soll Kund*innen neben den reinen Funktionsumfängen eines Produktes oder Services von dessen Value Proposition überzeugen. Unternehmen, welche einst als Datenkraken verpönt waren bemühen sich nun bewusst datensparsam und vertrauenswürdig aufzutreten. Kurz nach der Einführung der DSGVO wurde noch von einem Wettbewerbsvorteil gesprochen, wenn Datenschutzmaßnahmen besonders konsequent umgesetzt wurden. Heute lässt sich feststellen, dass es definitiv ein Wettbewerbsnachteil ist, wenn Datenschutzanforderungen nicht nachhaltig umgesetzt werden.

Fangen wir bei den offensichtlichen Risiken für einen Wettbewerbsnachteil an: Strafen und Bußgelder. Die potenziellen Kosten für die Ahndung von Datenschutzverstößen stehen in keinem Verhältnis zu den Investitionen für die Schaffung einer grundlegenden Datenschutz-Compliance. Dies gilt sowohl für die DSGVO als auch für Datenschutzgesetze in Drittstaaten. Hinzukommt, dass Strafen und Bußgelder einerseits mehrfach verhängt und andererseits auch verpflichtende Maßnahmen seitens Behörden auferlegt werden können, um erneute Verfehlungen zu verhindern.

Ein weiterer Grund, weshalb nachhaltiger Datenschutz notwendig ist, sind die Opportunitätskosten. Anders als physische Güter müssen Daten keine institutionalisierten Import- und Exportkontrollen durchlaufen. Binnen eines Wimpernschlags kann sich der Ort, an dem Daten verarbeitet werden, ändern. Damit geht analog physischer Güter auch eine Veränderung der rechtlichen Rahmenbedingungen einher. Um auf Marktentwicklungen, -chancen und -eintritte reagieren zu können, benötigen Unternehmen Flexibilität. Diese Flexibilität ist nicht gegeben, wenn die eigene Datenschutzorganisation nur unter der europäischen DSGVO eine Compliance sicherstellen kann.

Der dritte und unserer Meinung nach auch wichtigste Grund für einen nachhaltigen Datenschutz ist die Tatsache, dass regulatorische Entwicklungen der letzten Jahren nicht die Charakteristika eines zeitweiligen Trends aufweisen. Datenschutzregulierung hat seit der Einführung der DSGVO stark zugenommen. Zahlreiche Staaten haben neue Datenschutzgesetze verabschiedet oder bestehende Vorschriften erneuert. Daraus ergibt sich für den Moment ein komplexes Gemisch aus ähnlichen, aber auch teilweise sich widersprechenden Datenschutzanforderungen, mit welchen sich international tätige Unternehmen konfrontiert sehen. Langfristig ist eine Harmonisierung internationaler Datenschutzanforderungen sowohl aus Unternehmens- als auch Konsument*innensicht wünschenswert. Jedoch besteht jetzt der Bedarf für eine nachhaltige Datenschutz-Compliance, welche auf unterschiedliche Anforderungen reagieren kann und das Potenzial bietet, bereits etablierte Datenschutzlösungen für neue Regularien wiederzuverwenden.

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-Knowhow 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.

Capgemini invent

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.

Welche Unternehmen uns Rede und Antwort standen

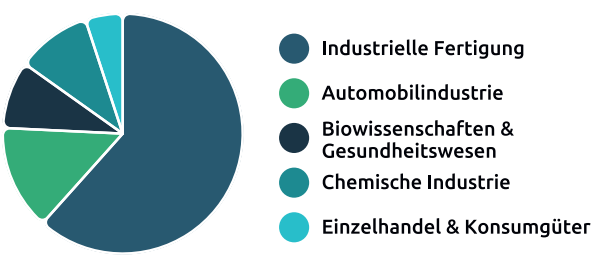
Methodisches Vorgehen

Für diese Studie wurden 75 ausgewählte Unternehmen in Österreich in einer quantitativen Befragung nach ihrer Selbsteinschätzung hinsichtlich der Erfüllung weltweiter Datenschutzgesetze und -vorschriften befragt. Die Auswahl der befragten Unternehmen wurde anhand der Unternehmensgröße sowie dem Internationalisierungsgrad getroffen. Unter Internationalisierungsgrad wurde hier der Vertrieb von Produkten und Services in Nicht-EU-Ländern verstanden. Neben der quantitativen Befragung wurden auch fünf qualitative Interviews mit ausgewählten Unternehmen durchgeführt. Hier wurde die Auswahl aufgrund der wirtschaftlichen Relevanz der jeweiligen Unternehmen getroffen. An der Studie nahmen ein Drittel der befragten Unternehmen teil. Dabei sind 62% der teilnehmenden Unternehmen in der industriellen Fertigung, 14% in der Automobilindustrie, 10% in der Chemieindustrie, 9% in der Biowissenschaft und im Gesundheitswesen, und 5% im Bereich Einzelhandel und Konsumgüter tätig.

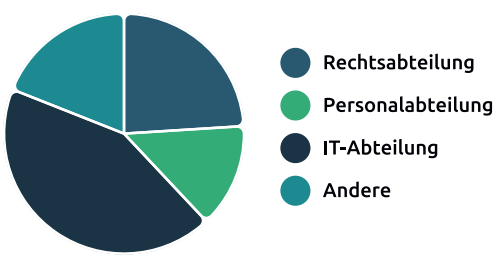
Quantitative Befragung
Die Befragung wurde mittels eines Online-Fragebogens durchgeführt. Im Rahmen der Befragung wurde darauf geachtet, dass nur Entscheidungsträger mit einem fortgeschrittenen Datenschutzwissen teilnehmen. Der Fragebogen selbst wurde in sechs Abschnitte gegliedert und enthielt neben allgemeinen Fragen zur Unternehmenseinordnung, die fünf Bausteine der zwei Dimensionen Datenschutzkultur und Datenschutz-Compliance, die sich auch in dieser Studie als strukturgebendes Element wiederfinden.

Qualitative Interviews
Die Interviews wurden persönlich mit den Ansprechpersonen der Unternehmen durchgeführt. Dabei wurden in den Interviews die Themen der Befragung aufgegriffen und zwischen den Gesprächsteilnehmer*innen fachlich diskutiert. Die Ergebnisse aus den Interviews haben es uns ermöglicht, Antworten besser interpertieren und mögliche Problemstellungen der Unternehmen herausarbeiten zu können.

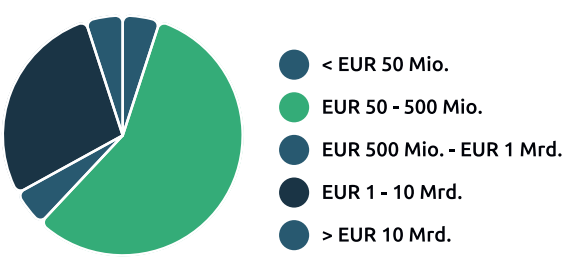
In welchen Industrien sind befragte Unternehmen tätig?



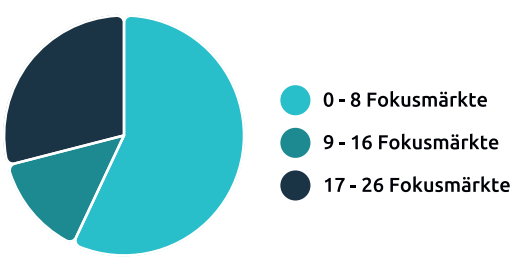
Welchen Abteilungen gehören befragte Datenschutzexpert*innen an?



Wie hoch ist der Jahresumsatz befragter Unternehmen?



In wie vielen Fokusmärkten sind befragte Unternehmen tätig?



Vielen Dank für Ihr Interesse an unserer Studie

Über die Autoren

Simon El Dib
Senior Director
Enterprise Transformation | Capgemini Invent

simon.el-dib@capgemini.com

Simon leitet seit 2017 erfolgreich Capgemini Invent in Österreich. Gemeinsam mit den Kolleg*innen am Standort Wien unterstützt er Kunden bei diversen Transformationsprojekten. Einen besonderen Fokus hat Simon auf Projekte im Manufacturing-Umfeld gerichtet. Dabei schätzen seine Kunden die pragmatischen Ansätze.

Benjamin Wirtz
Senior Manager
Business Technology | Capgemini Invent

benjamin.wirtz@capgemini.com

Ben und sein Team unterstützen unsere Kunden bei den datenschutzrechtlichen Herausforderungen, die mit dem wachsenden Angebot von digitalen Produkten und Services immer komplexer werden. In seinen Datenschutzprojekten legt er besonderen Fokus auf internationale Projektteams. So können lokale Datenschutzherausforderungen durch internationale Zusammenarbeit und globale Ansätze bewältigt werden.

Fabian Sünkler
Senior Consultant
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 internationaler Datenschutzrichtlinien verlangt daher nach modularen Lösungen.

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 10,000+ 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 340,000 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 2021 global revenues of €18 billion.

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