# Globale Datenschutzbestimmungen

Die Gesellschaft, in der wir als Privatpersonen oder Unternehmer leben, ist zunehmend digitalisiert. Tatsächlich hat sich die Nutzung von digitalen Tools und des Internets in vielen Bereichen stark demokratisiert, was zahlreiche Veränderungen zur Folge hatte und neue Konsum- und Interaktionsmuster auslöste.

Viele Daten werden heute digitalisiert, in Computersystemen gespeichert und online zur Verfügung gestellt. Der Datenschutz ist daher von entscheidender Bedeutung für den Schutz der Nutzerinnen und Nutzer. Um wettbewerbsfähig zu bleiben, waren die Unternehmen gezwungen, neue Technologien zu integrieren, aber auch die neuen rechtlichen Rahmenbedingungen einzuhalten. Das Thema Datenschutz ist heutzutage sowohl entscheidend als auch strategisch, um den Fortbestand eines Unternehmens zu sichern und seinen Ruf zu stärken.

Daher ist es für Unternehmen unabdingbar, die rechtlichen Rahmenbedingungen für den Datenschutz auf der ganzen Welt zu verstehen, um diese einzuhalten. Dieser Leitfaden bietet Unternehmen einen Überblick über die verschiedenen Regelungen zum Datenschutz. Er erhebt keinen Anspruch auf Vollständigkeit.

## Was ist Datenschutz und warum sollte er geregelt werden?

Die Datenschutzgesetze schützen die Grundrechte und die Persönlichkeit natürlicher Personen. Deren Hauptzweck ist der Schutz von Personen und nicht der Schutz der Daten selbst. Datenschutz bezieht sich auf die Praxis, persönliche und sensible Daten von Privatpersonen oder Organisationen vor unbefugtem Zugriff, Nutzung, Offenlegung oder Veränderung zu sichern und zu bewahren. Er soll die Vertraulichkeit, Integrität und Verfügbarkeit von Daten gewährleisten und gleichzeitig die Grundrechte auf Privatsphäre und Datenschutz wahren.

### Personenbezogene Daten dürfen nicht mit sensiblen Daten verwechselt werden

Nach dem Datenschutzgesetz (DSG) beziehen sich **personenbezogene Daten** auf alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

Sensible **personenbezogene Daten** umfassen Daten über religiöse, philosophische, politische oder gewerkschaftliche Meinungen oder Aktivitäten, Daten zur Gesundheit, Intimsphäre oder Rasse oder ethnische Herkunft, genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Daten über strafrechtliche und administrative Verfolgungen oder Sanktionen und Daten über Massnahmen sozialer Hilfe.



REPUBLIQUE ET CANTON DE GENEVE
POST TENEBRAS LUX

h e g
Haute école de gestion Genève

UNIVERSITÉ DE GENÈVE

Erfahren Sie mehr

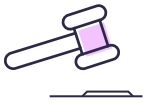
# Herausforderungen beim Datenschutz

- **Rechte der Einzelperson**
  Einzelpersonen das Recht garantieren, ihre persönlichen Daten zu korrigieren, auf sie zuzugreifen und sie zu berichtigen.

- **Wachsende Bedrohungen**
  Mit der zunehmenden Digitalisierung sind die Risiken für Datenverletzungen gestiegen. Dazu gehören Zerstörung, Verlust, Veränderung, Offenlegung und unbefugter Zugriff, wie z. B. Hacking.

- **Vertrauen der Kunden**
  Stärkung des Vertrauens von Kundinnen und Kunden sowie Partnern in Unternehmen, da sie wissen, dass ihre Daten sicher verarbeitet werden.

- **Verantwortung von Unternehmen**
  Die Unternehmen sind verpflichtet, angemessene Sicherheitsvorkehrungen zu treffen und transparent zu machen, wie sie die Daten nutzen.



- **Sanktionen**
  Bei Nichteinhaltung können Unternehmen und/oder Privatpersonen mit hohen Geldstrafen belegt werden, wodurch die Bedeutung der Einhaltung von Vorschriften noch weiter steigt.

- **Internationale Harmonisierung**
  Die Vorschriften helfen dabei, gemeinsame Standards für den grenzüberschreitenden Schutz von Daten festzulegen, und erleichtern so den internationalen Informationsaustausch.

## Bundesgesetz über den Datenschutz (DSG)

Das **Bundesgesetz über den Datenschutz (DSG)** ist das Datenschutzgesetz der Schweiz. Das erste DSG stammt aus dem Jahr 1992. Insbesondere mit dem Aufkommen des Internets wurde eine umfassende Revision des DSG notwendig, um der Bevölkerung einen angemessenen Schutz ihrer Daten zu gewährleisten, der an die jüngsten technologischen Entwicklungen angepasst ist. Eine Revision dieses Gesetzes war auch unerlässlich, damit das Schweizer Recht weiterhin mit dem europäischen Recht und insbesondere der **Allgemeinen Datenschutzverordnung (DSGVO)** vereinbar ist. Dadurch wird der freie Datenverkehr mit der Europäischen Union gewährleistet.

Das neue DSG trat am 1. September 2023 mit sofortiger Wirkung in Kraft und ersetzte das alte Gesetz aus dem Jahr 1992 vollständig. Es zielt darauf ab, die Verarbeitung personenbezogener Daten zu verbessern und gewährt den Schweizer Bürgerinnen und Bürgern neue Rechte, bringt aber auch eine Reihe von Verpflichtungen für Unternehmen mit sich.

Die Ausführungsbestimmungen zum Gesetz, die in der neuen **Datenschutzverordnung (DSV)** und der **Verordnung über Datenschutzzertifizierungen (VDSZ)** verankert sind, traten gleichzeitig mit dem DSG am 1. September 2023 in Kraft.

**Die sieben Grundsätze für den Datenschutz**

- Rechtmässigkeit
- Treu und Glauben
- Verhältnismässigkeit
- Zweck
- Richtigkeit
- Sicherheit
- Transparenz

# Ein wenig Geschichte

**19. Juni 1992**
Inkrafttreten des Bundesgesetzes über den Datenschutz (DSG).

**24. Juni 1976**
Verabschiedung des Gesetzes über automatisch verarbeitete Informationen (LITAO).

**25. Mai 2018**
Inkrafttreten der Allgemeinen Datenschutzverordnung (DSGVO)

**1. März 2019**
Teilrevision des Bundesgesetzes über den Datenschutz (DSG).

**25. August 2023**
Inkrafttreten der EU-Verordnungen über digitale Dienste (Digital Services Act, DSA) und den digitalen Markt (Digital Market Act, DMA) für grosse Plattformen.

**1. September 2023**
Inkrafttreten des neuen Bundesgesetzes über den Datenschutz (DSG).

**17. Februar 2024**
Inkrafttreten der EU-Verordnungen über digitale Dienste (Digital Services Act, DSA) und den digitalen Markt (Digital Market Act, DMA) für kleinere Plattformen.

# Unternehmen, die unter das Datenschutzgesetz fallen

**Alle Unternehmen, die in der Schweiz tätig sind oder in der Schweiz Auswirkungen entfalten, fallen darunter und sind verpflichtet, sich unverzüglich an die neuen Datenschutzbestimmungen anzupassen.**

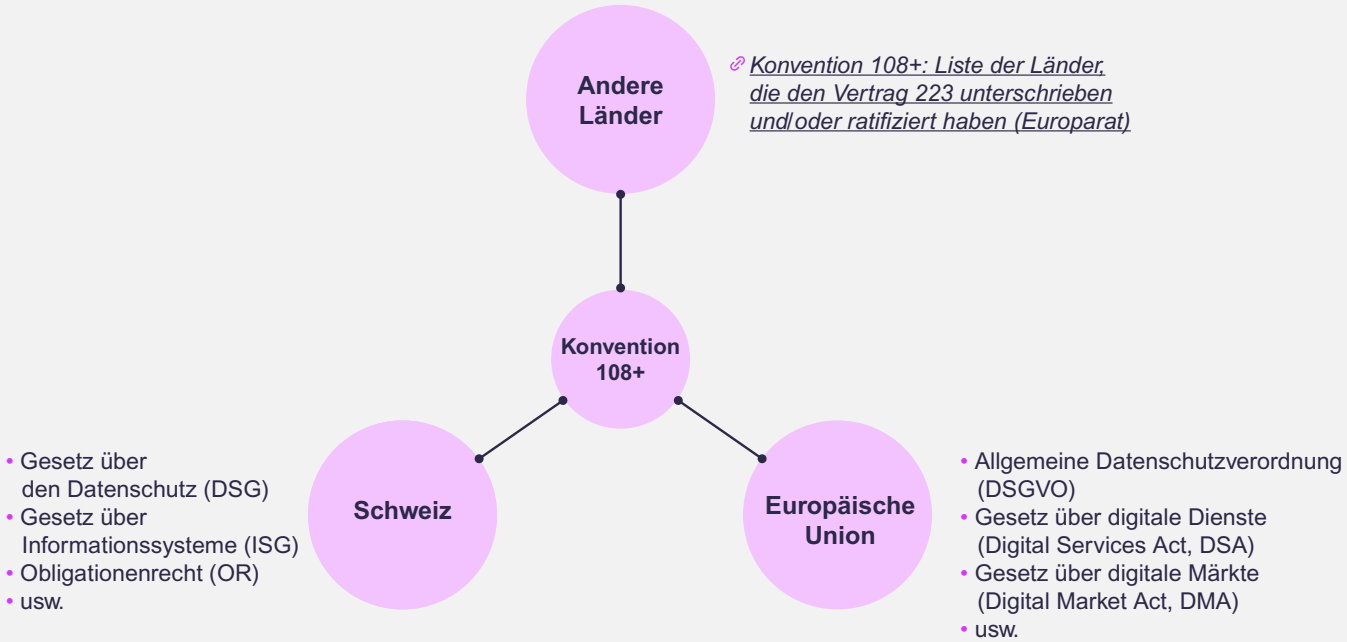
### Die Schweiz und die 108+ Konvention

Obwohl die Schweiz nicht Mitglied der Europäischen Union ist, unterschrieb sie die Konvention 108+ und verpflichtete sich damit, ähnliche Praktiken wie die anderen Staaten, die dieses Übereinkommen ratifiziert haben, in Bezug auf die Verarbeitung personenbezogener Daten einzuführen.

Die Konvention 108+ ist ein vom Europarat erstellter Vertrag über den Schutz der Daten von Privatpersonen bei der automatisierten Verarbeitung ihrer persönlichen Daten. Ihr Ziel ist es, die Richtlinien für den Datenschutz festzulegen, um sicherzustellen, dass die Rechte und Freiheiten von Privatpersonen, insbesondere ihre Privatsphäre, bei der Nutzung ihrer Informationen berücksichtigt werden.

Die Konvention 108 wurde 1981 eingeführt und war das erste rechtsverbindliche internationale Instrument. Eine Aktualisierung erfolgte 2018 unter der Bezeichnung Konvention 108+. Diese Aktualisierung stärkt die Rechte des Einzelnen und modernisiert die Grundsätze des Datenschutzes im digitalen Zeitalter, insbesondere durch einen besseren Schutz vor den Risiken, die mit der automatisierten Verarbeitung verbunden sind.

Die Konvention 108+ steht Staaten offen, die nicht Mitglieder des Europarats sind. Sie entfaltet somit auch aussereuropäisch ihre Wirkung.




*Konvention 108+: Liste der Länder, die den Vertrag 223 unterschrieben und/oder ratifiziert haben (Europarat)*

# Die Notwendigkeit, die gesetzlichen Rahmenbedingungen für den Schutz personenbezogener Daten einzuhalten

In den meisten Ländern wurden die Datenschutzbestimmungen entwickelt, um die Interessen sowohl von Einzelpersonen als auch von Unternehmen vor den schädlichen Folgen einer unregulierten Nutzung persönlicher Daten zu schützen. Diese Vorschriften regeln nicht nur die Verwendung von Daten, um die Rechte von Privatpersonen zu gewährleisten, sondern legen im weiteren Sinne Grundsätze und bewährte Verfahren für die Erhebung, Verarbeitung und Verwaltung von Daten fest. So stellen sie sicher, dass Unternehmen und Privatpersonen, die mit Daten zu tun haben, die Vertraulichkeit wahren und die Informationen sicher und ethisch korrekt nutzen. In der Schweiz ist zu beachten, dass das DSG natürliche Personen, nicht aber juristische Personen schützt.

**Infrastruktur kann teuer sein!**
Je nach betroffenem Land, der Schwere der Tat und den Vorschriften können hohe Geldstrafen verhängt werden, die von einigen Tausend Franken bis zu mehreren Millionen Franken reichen.

In der Schweiz betreffen die Sanktionen des DSG natürliche Personen mit einer Obergrenze von 250.000 CHF. Wenn mit verhältnismässigem Aufwand kein Verursacher gefunden werden kann, sieht das DSG eine subsidiäre Bussgeldpflicht für Unternehmen in der Höhe von maximal 50.000 CHF vor.

Die Geldstrafen in der Europäischen Union sind wesentlich höher; es können Sanktionen in Höhe von bis zu 20 Millionen Euro oder im Falle eines Unternehmens bis zu 4% des weltweiten Jahresumsatzes verhängt werden.

Die Einhaltung der Datenschutzbestimmungen ist nicht nur zur Vermeidung rechtlicher Risiken, sondern auch für die nachhaltige Entwicklung und den Betrieb des Geschäfts von entscheidender Bedeutung. Digitales Vertrauen ist eine strategische Herausforderung für Unternehmen, um sich auf dem Markt zu differenzieren, das Vertrauen der Kunden zu bewahren und auszubauen und den Wohlstand des Unternehmens zu sichern.

***„Das Datenschutzgesetz führt neue Verpflichtungen für Unternehmen ein, verspricht aber auch, völlig neue wirtschaftliche Möglichkeiten zu eröffnen, die Innovation und sektorales Wachstum begünstigen.“***

Dessislava Leclère, Lehrbeauftragte an der höheren Wirtschafts- und Verwaltungsschule Genf (Haute École de Gestion de Genève, HEG)

# Die Notwendigkeit, die gesetzlichen Rahmenbedingungen für den Schutz personenbezogener Daten einzuhalten

Die Einhaltung der Vorschriften bedeutet auch viele Chancen für Unternehmen:

- Eine Investition in den Datenschutz ist eine Investition in die Cybersicherheit des eigenen Unternehmens. Durch die Bereitstellung angemessener Ressourcen für die Datensicherheit und die Sicherheit von Informationssystemen können Unternehmen ihre Widerstandsfähigkeit gegenüber digitalen Bedrohungen und Risiken erhöhen.
- Durch die Gewährleistung der Vertraulichkeit, Integrität und Verfügbarkeit von Daten stärkt und entwickelt das Unternehmen seinen Ruf und das Vertrauen bei seinen Kunden, Partnern und Mitarbeitern.
- Die Einhaltung der Richtlinien schützt ein Unternehmen vor den Folgen, die zu einem Vertrauensverlust innerhalb der Organisation, bei Kunden oder Partnern führen können, wie schlechte Werbung und negative Berichterstattung in den Medien, Probleme bei der Einstellung von Mitarbeitern und sinkende Attraktivität, sofern das Unternehmen als nachlässig in Bezug auf Sicherheit, Ethik und Datenschutz wahrgenommen wird.
- Durch die Einhaltung der rechtlichen Rahmenbedingungen und die Antizipation von Risiken im Zusammenhang mit dem Datenschutz kann ein Unternehmen den Marktzugang aufrechterhalten und neue Märkte erschliessen. Dadurch wird das Risiko vermieden, von öffentlichen Aufträgen ausgeschlossen zu werden, die Zusicherungen zur Einhaltung von Datenschutzbestimmungen und -praktiken erfordern.
- Ein verantwortungsbewusstes und transparentes Vorgehen gegenüber seinen Interessengruppen ermöglicht es einem Unternehmen, sein Handeln und seine Werte zu fördern und sich so von der Konkurrenz abzuheben.
- Durch die Einführung angemessener Massnahmen für das digitale Risikomanagement beugt das Unternehmen finanziellen Risiken vor. Diese Risiken können die Folgenden sein: Hohe Geldstrafen, Kosten für die Wiedergutmachung von Schäden, die den Beteiligten entstanden sind, Kosten für die Durchführung von Korrekturmassnahmen nach einem Vorfall, höhere Versicherungsprämien, Wertverlust von Vermögenswerten wie Kundendatenbanken, wenn diese gestohlen werden usw.
- Es können verschiedene betriebliche und technische Risiken auftreten, die zu einer Unterbrechung des gesamten oder eines Teils des Geschäftsbetriebs führen, Auswirkungen auf den operativen und geschäftlichen Betrieb des Unternehmens haben und das Risiko von Cyberangriffen erhöhen, wenn keine präventiven und normativen Massnahmen ergriffen werden.
- Durch die Einhaltung der geltenden rechtlichen Rahmenbedingungen vermeidet das Unternehmen rechtliche und vertragliche Risiken, wie das Risiko, von Kunden, Partnern oder sogar Regierungen verklagt zu werden, sowie mögliche Einschränkungen oder Verbote der Verarbeitung bestimmter Daten. Damit übernimmt das Unternehmen auch die Verantwortung dafür, dass seine Auftragnehmer die rechtlichen Rahmenbedingungen einhalten. Das Unternehmen muss daher sicherstellen, dass die Einhaltung der Gesetze für sich selbst und seine Auftragnehmer gewährleistet ist.

**Datenschutzbeauftragter**

Der kantonale Datenschutz- und Öffentlichkeitsbeauftragte (KDÖB) überwacht die Anwendung des kantonalen Datenschutz- und Öffentlichkeitsgesetzes. In Genf handelt es sich um das Gesetz über die Information der Öffentlichkeit, den Zugang zu Dokumenten und den Schutz personenbezogener Daten (LIPAD), das für den öffentlichen Sektor in Genf gilt.

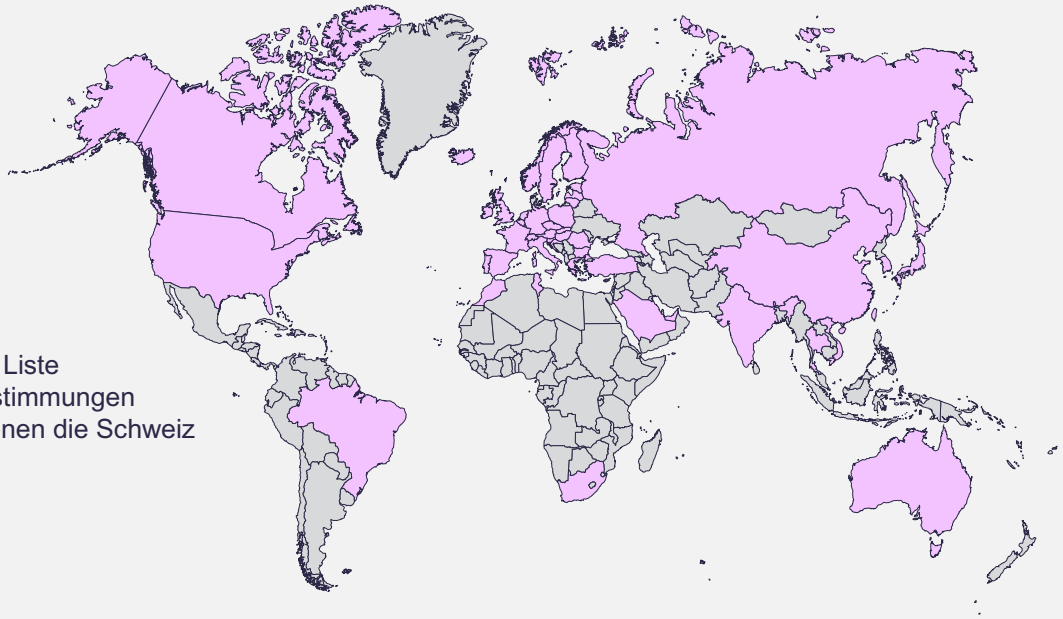
Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) ist für die Überwachung der korrekten Anwendung der eidgenössischen Datenschutzbestimmungen zuständig. Er überwacht insbesondere die Verarbeitung von Daten durch Unternehmen. Er ist auch die Schlichtungsstelle für den Zugang zu amtlichen Dokumenten.

# Regulatorische Rahmenbedingungen weltweit

**Angesichts der Tatsache, dass täglich viele Daten online ausgetauscht werden, wird die Notwendigkeit, die Privatsphäre zu schützen und die Sicherheit der Daten zu gewährleisten, in vielen Ländern immer wichtiger.**

**Laut der Konferenz der Vereinten Nationen für Handel und Entwicklung (UNCTAD) hatten Ende 2021 von 194 Ländern 137 eine direkte oder indirekte Regulierung für den Schutz von Daten und der Privatsphäre eingeführt.**

Nicht erschöpfende Liste der Datenschutzbestimmungen von Ländern, mit denen die Schweiz Handel treibt.



| | | |
|---|---|---|
| **Schweiz** | Loi sur la protection des données (LPD) / Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG) / Nuova legge sulla protezione dei dati (LPD) | 2023 |
| **Europäische Union** | Règlement général sur la protection des données (RGPD) | 2018 |
| **Vereinigtes Königreich** | UK General Data Protection Regulation | 2021 |
| **Norwegen** | Personvernforordningen GDPR | 2021 |
| **Island** | Almenna persónuverndarreglugerði | 2018 |
| **Türkei** | Kişisel verilerin korunmasi kanunu | 2016 |
| **Vereinigte Staaten** | Lois spécifiques par État | 2020 |
| **Kanada** | Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE) | 2020 |
| **Brasilien** | Lei Geral de Proteção de Dados Pessoais | 2020 |
| **Tunesien** | Loi sur la protection des données à caractère personnel | 2004 |
| **Marokko** | Loi relative à la protection des données des personnes physiques à l'égard des traitements des données à caractère personnel | 2009 |
| **Südafrika** | The Protection of Personal Information Act (POPIA) | 2020 |
| **Vereinigte Arabische Emirate** | القانون الاتحادي بشأن حماية البيانات الشخصية | 2021 |
| **Russland** | О персональных данных | 2006 |
| **Indien** | Information Technology Act | 2020 |
| **China** | Personal information protection law (PIPL) | 2021 |
| **Hongkong** | Personal Data (Privacy) Ordinance | 1996 |
| **Japan** | 個人情報の保護に関する法律 | 2017 |
| **Südkorea** | 개인정보 보호법 | 2011 |
| **Taiwan** | Personal Data Protection Act | 2015 |
| **Singapur** | Personal Data Protection Act | 2012 |
| **Thailand** | พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล | 2019 |
| **Vietnam** | Nghị định bảo vệ dữ liệu cá nhân (Nghị định BVDLCN) | 2023 |
| **Australien** | Privacy Act | 1988 |

# Verpflichtungen in Bezug auf verschiedene Datenschutzbestimmungen

| | |
|---|---|
| **Staaten, in denen ein angemessenes Schutzniveau für Daten gewährleistet ist** | Bewertung der Angemessenheit des Schutzniveaus, einschliesslich der Übermittlung von Daten. *Datenschutzverordnung (DSGVO)* |
| **Informationspflicht** | Alle Unternehmen sind verpflichtet, den betroffenen Personen und/oder Stellen die Zwecke, Quellen und Methoden der Verarbeitung personenbezogener Daten klar und transparent mitzuteilen. |
| **Register der Aktivitäten** | Unternehmen sind verpflichtet, ein Register ihrer Aktivitäten zu führen, in dem alle Vorgänge, bei denen personenbezogene Daten verarbeitet werden, verzeichnet sind. |
| **Folgenabschätzung** | Je nach Kategorie der von Unternehmen verarbeiteten Daten müssen sie eine Folgenabschätzung über die Risiken einer Verarbeitung personenbezogener Daten durchführen, um deren Schutz zu gewährleisten. |
| **Einwilligung bei der Verarbeitung sensibler Daten** | Je nach Art der Verarbeitung und der verarbeiteten Daten müssen Unternehmen die ausdrückliche und informierte Einwilligung der Personen, deren Daten sie verarbeiten, einholen. |
| **Meldung von Verstössen gegen den Schutz personenbezogener Daten** | Unternehmen sind verpflichtet, die Behörden und möglicherweise auch die betroffenen Personen zu informieren, wenn eine Sicherheitsverletzung zum Zugriff, zur Offenlegung oder zum Verlust persönlicher Daten führt. |
| **Privacy by Design/by Default** | Unternehmen müssen den Datenschutz bereits bei der Konzeption eines Produkts oder einer Dienstleistung integrieren (Privacy by Design). Darüber hinaus müssen die Standardeinstellungen von Diensten oder Software das höchste Datenschutzniveau und die höchste Sicherheit ohne Eingreifen des Nutzers gewährleisten (Privacy by Default). |
| **Anwesenheit eines Datenschutzbeauftragten** | Unternehmen sind verpflichtet, eine Person zu ernennen, die für den Schutz personenbezogener Daten verantwortlich ist (Datenschutzbeauftragter), um die Einhaltung der geltenden Vorschriften zu gewährleisten. |
| **Sanktionen** | Bei Verstössen gegen die Datenschutzgesetze drohen Unternehmen Bussgelder. |
| **Recht auf Transparenz für Einzelpersonen** | Unternehmen müssen Einzelpersonen darüber informieren, wie ihre persönlichen Daten gesammelt, genutzt und weitergegeben werden. |
| **Zugangsrecht** | Unternehmen sind verpflichtet, Personen auf Anfrage eine Kopie der bei ihnen gespeicherten personenbezogenen Daten zur Verfügung zu stellen. |
| **Recht auf Berichtigung** | Unternehmen sind verpflichtet, ungenaue oder unvollständige personenbezogene Daten, über die sie verfügen, auf Anfrage einer Einzelperson zu korrigieren oder zu aktualisieren. |
| **Recht auf Löschung** | Unternehmen sind verpflichtet, die personenbezogenen Daten von Einzelpersonen zu löschen, wenn diese sie dazu auffordern. |
| **Recht auf Einschränkung der Verarbeitung** | Unter bestimmten besonderen Umständen müssen Unternehmen die Verarbeitung der Daten einer Person vorübergehend einschränken, wenn diese Person sie dazu auffordert. |
| **Recht auf Übertragbarkeit** | Unternehmen sind verpflichtet, Einzelpersonen auf Anfrage ihre personenbezogenen Daten in einem gängigen nutzbaren Format zu übermitteln und sie auf Wunsch an ein anderes Unternehmen weiterzuleiten. |
| **Recht auf Widerspruch** | Unternehmen müssen Einzelpersonen die Möglichkeit geben, der Verarbeitung ihrer personenbezogenen Daten aus legitimen Gründen zu widersprechen. |
| **Recht, nicht Gegenstand einer vollautomatisierten Entscheidung zu sein** | Einzelpersonen können von Unternehmen verlangen, dass eine automatisierte Verarbeitung ihrer Daten, die zu einer Entscheidung führt, von einer Einzelperson überprüft wird. |

# Vergleichstabelle

| | Schweiz | Europäische Union | Vereinigtes Königreich | Norwegen | Island | Türkei | Vereinigte Staaten | Kanada | Brasilien | Tunesien | Marokko | Südafrika | Vereinigte Arabische Emirate | Russland | Indien | China | Hongkong | Japan | Südkorea | Taiwan | Singapur | Thailand | Vietnam | Australien |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Staaten, in denen ein angemessenes Schutzniveau für Daten gewährleistet ist **(Link hier)** | ● | ● | ● | ● | ● | | | ● | | | | | | | | | | | | | | | | |
| Informationspflicht | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ○ | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| Register der Aktivitäten | ● | ● | ● | ● | ● | ● | ○ | ● | ● | ● | ● | ● | | | | | | | ○ | | | ○ | ● | |
| Folgenabschätzung | ● | ● | ● | ● | ● | ○ | ○ | ● | ● | | | ● | ○ | ○ | ○ | ● | | | | | | | ● | |
| Einwilligung zur Verarbeitung sensibler Daten | ● | ● | ● | ● | ● | ● | ○ | ● | ● | ● | ● | ● | ● | ● | | ● | ○ | ● | ● | ● | ● | ● | ● | ● |
| Meldung von Verstössen gegen den Schutz personenbezogener Daten | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | | | ● | ● | ● | ● | ● | ● |
| Privacy by Design/ by Default | ● | ● | ● | ● | ● | ○ | ○ | ● | ○ | | | | | | | | | | | | | | ● | |
| Anwesenheit eines Datenschutzbeauftragten | ○ | ● | ● | ● | ● | ○ | ○ | ● | ● | ○ | ○ | ● | ○ | ○ | ○ | ● | | | ● | | ● | ○ | ○ | |
| Sanktionen | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| Recht auf Transparenz für Einzelpersonen | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| Zugangsrecht | ● | ● | ● | ● | ● | ● | ○ | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | | ● | ● | ● | ● | ● | ● |
| Recht auf Berichtigung | ● | ● | ● | ● | ● | ● | ○ | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| Recht auf Löschung | ● | ● | ● | ● | ● | ● | ○ | ● | ● | ● | ○ | ● | ● | ● | ○ | ○ | ○ | ● | ● | ○ | ○ | ● | ● | ○ |
| Recht auf Einschränkung der Verarbeitung | ● | ● | ● | ● | ● | ● | ○ | ● | ● | ● | | ● | ● | | | ● | | ○ | ● | | | ● | ● | |
| Recht auf Übertragbarkeit | ● | ● | ● | ● | ● | | ○ | | ● | ● | | | ● | | | ● | | | ● | | | ● | ● | |
| Recht auf Widerspruch | ● | ● | ● | ● | ● | ● | ○ | ● | ● | ● | ● | ● | ● | | ● | ● | ○ | ○ | ● | | ● | ● | ● | |
| Recht, nicht Gegenstand einer vollautomatisierten Entscheidung zu sein | ● | ● | ● | ● | ● | ○ | ○ | ● | ● | ● | | ○ | ● | ○ | | ○ | | | ● | | | | | |

● = *Ja*
○ = *Ja in bestimmten Fällen, Staaten oder Provinzen*

*Beziehen Sie sich immer auf die geltenden Vorschriften. Diese Daten sind unverbindlich.*
*Sie sollten die Informationen immer sicherstellen, indem Sie die Vorschriften des jeweiligen Landes lesen.*

# Schritte zur optimalen Verwaltung von Daten und zur Einhaltung von Vorschriften

**Identifizierung der Märkte, in denen das Unternehmen tätig ist.** Zunächst sollten die Länder, Regionen oder Staaten aufgelistet werden, in denen das Unternehmen tätig ist. Anschliessend muss festgestellt werden, welche Arten von Geschäfts- oder Managementtätigkeiten das Unternehmen in diesen Regionen ausübt und ob diese den geltenden Vorschriften unterliegen.

**Lesen und Verstehen der geltenden Vorschriften in den Ländern, in denen das Unternehmen tätig ist.** Die rechtlichen Rahmenbedingungen unterscheiden sich je nach Region und der Art der Geschäftstätigkeit der Unternehmen. Es ist unerlässlich, sich über die geltenden Bestimmungen in den Ländern, in denen das Unternehmen tätig ist, zu informieren, um die geltenden Gesetze einzuhalten.

**Nur notwendige Daten erfassen.** Es muss sichergestellt werden, dass die Datenverarbeitung rechtmässig ist. Die Datenerhebung muss auf das absolut Notwendige minimiert werden, indem man sich auf den Zweck der Verarbeitung beschränkt, der vom Unternehmen vereinbart und bei der Datenerhebung angekündigt wurde. Zudem muss festgelegt werden, wie lange diese Informationen aufbewahrt werden müssen.

**Inventarisierung und Kartierung der Daten, die sich im Besitz des Unternehmens befinden**. Diese Bestandsaufnahme ermöglicht es, mögliche Informationen zu identifizieren, über die das Unternehmen nicht verfügen sollte, um die Vorschriften einzuhalten und den erforderlichen Umgang mit diesen Daten zu praktizieren.

**Verwaltung des Lebenszyklus von Daten.** Es ist wichtig, festzulegen, wie lange die erhobenen oder erzeugten Daten benötigt werden, und ein Datum zu vereinbaren, an dem die Daten gelöscht werden. Wenn die Daten für die Zwecke der Verarbeitung nicht mehr erforderlich sind, müssen sie vernichtet oder anonymisiert werden.

**Entwicklung und Umsetzung einer Politik der Transparenz bei der Verarbeitung von Daten**. Wie bei der Erhebung von Daten ist es auch hier unerlässlich, transparent zu machen, welche Daten vorhanden sind, zu welchem Zweck sie verarbeitet werden und wie sie vom Unternehmen oder seinen Partnern genutzt werden sollen.

**Schutz von Daten.** Es ist wichtig, alle notwendigen Massnahmen zu ergreifen, um die Daten, die sich im Besitz des Unternehmens befinden und von diesem verwaltet werden, zu schützen. Dies betrifft insbesondere technische Massnahmen und die Schulung aller Personen, die Zugang zu den Daten haben.

*Weitere Informationen finden Sie im Leitfaden „Cyberrisiken“.*

**Genf als Pionierkanton für das Recht auf digitale Integrität**

Am 18. Juni 2023 stimmten die Genferinnen und Genfer mit 94,21% der Änderung der Verfassung der Republik und des Kantons Genf zu, um ein Grundrecht zum Schutz der digitalen Integrität der Bürgerinnen und Bürger einzuführen, das hauptsächlich im Rahmen ihrer Beziehungen zu den öffentlichen Verwaltungen gelten soll.