MORGENSTERN

# Whitepaper

## Das revidierte Schweizer Datenschutzgesetz

# Inhaltsübersicht

Wir bei MORGENSTERN legen grossen Wert auf inklusive Sprache. Deswegen gendern wir – und zwar gerne! Sie sollen sich von unseren Texten angesprochen fühlen, egal wer Sie sind. Fachbegriffe gendern wir jedoch nicht, da sie wie Eigennamen feststehende Begriffe sind. Hier geht es nicht um das generische Maskulinum, sondern um fachliches Vokabular, das seine eigene juristische Bedeutung hat.

...Ihnen aber nun **viel Spass**, liebe*r Leser*in!

## I. Einführung

Die digitale Welt hat sich in den letzten 20 Jahren rasant entwickelt. Die Covid-Pandemie mit einhergehendem Home-Office, Online-Shopping und Online-Datentransfers hat hierzu ihr Übriges getan. Entsprechend ist das Schutzbedürfnis der Privatperson vor Datenmissbrauch gestiegen.

Der Schutz dieses Bedürfnisses nach informationeller Selbstbestimmung, welche nur bei einem transparenten Umgang mit Daten umsetzbar ist, muss durch einen gesetzlichen Rahmen gewährleistet werden. Entsprechend hat die EU die DS-GVO erlassen und damit ein Schutzniveau geschaffen, welches der digitalen Realität der Zeit gerecht wird.

In der Herbstsession 2020 hat das Eidgenössische Parlament das totalrevidierte Bundesgesetz über den Datenschutz (revDSG) sowie weitere, geänderte Erlasse zum Datenschutz wie die Datenschutzverordnung (DSV) und die neue Verordnung über Datenschutzzertifizierungen (VDSZ) verabschiedet. Der Bundesrat hat am 31. August 2022 entschieden, das neue Datenschutzgesetz und die zugehörigen Verordnungen auf den 01. September 2023 ohne Übergangsfrist in Kraft zu setzen. Bis zum Inkrafttreten müssen die Privatwirtschaft und die Bundesbehörden die Bearbeitung von Personendaten an die neuen Bestimmungen anpassen. Damit wird die Schweiz bezüglich des Schutzniveaus mit der EU gleichziehen und seine Wettbewerbsfähigkeit sichern.

Dieses revDSG wird an Unternehmen in und ausserhalb der Schweiz einige Herausforderungen stellen. Das rechtskonforme Verfahren mit Personendaten wird künftig komplizierter und bürokratischer werden, jedoch auch datenschutzsicherer und transparenter.

Mit unserem Whitepaper revDSG geben wir Ihnen einen ersten Überblick über die neue Rechtslage, die Herausforderungen und Unterschiede zum „alten" DSG. Dieses Whitepaper soll Ihnen den Einstieg in die Materie erleichtern und ein erstes Grundverständnis schaffen. Bitte beachten Sie, dass dieses Whitepaper keinen Anspruch auf Vollständigkeit erhebt und keinesfalls eine Rechtsberatung und Prüfung im jeweiligen Fall ersetzt.

Wir bei MORGENSTERN unterstützen Sie gern bei der Umsetzung der neuen Anforderungen in Ihrem Unternehmen oder Ihrer Bundesbehörde.

contact@morgenstern-privacy.ch
+41 55 415 70 70

Hier geht's direkt zur Leistungsübersicht rund um das Thema revDSG.

MORGENSTERN

## II. Zielsetzung, Wirkungsbereich und Inkrafttreten des revDSG

### 1. Warum wurde das DSG revidiert?

Ziel der Revision des Bundesgesetzes über den Datenschutz (DSG) ist es, dieses an die veränderten technologischen und gesellschaftlichen Verhältnisse anzupassen. Hier stehen vor allem die Transparenz von Datenbearbeitungen und die Selbstbestimmung der betroffenen Personen über ihre Daten im Fokus. Darüber hinaus soll sich das DSG vom Niveau an die Anforderungen der DS-GVO der EU annähern, um weiterhin die Anerkennung der Schweiz als Drittstaat mit angemessenem Datenschutzniveau und damit die grenzüberschreitende Datenübermittlung auch für die Zukunft zu gewährleisten.

### 2. Für wen gilt das revDSG überhaupt?

Das revDSG soll die Persönlichkeit und Grundrechte natürlicher Personen schützen, die sich in der Schweiz befinden und deren Daten durch Private / den Staat bearbeitet werden. Die Daten juristischer Personen sind folglich nicht mehr geschützt. Wesentlich ist, wo sich die Datenbearbeitung „auswirkt" („Auswirkungsprinzip / Marktortprinzip"), also nicht unbedingt, wo sie veranlasst wird bzw. wo das bearbeitende Unternehmen / die bearbeitende Person ihren Sitz hat. Im Einzelfall kann die Feststellung, wo die „Auswirkung" (als Ausrichtung der Bearbeitung) zu verorten ist, schwerfallen. Hier helfen wir gerne weiter.

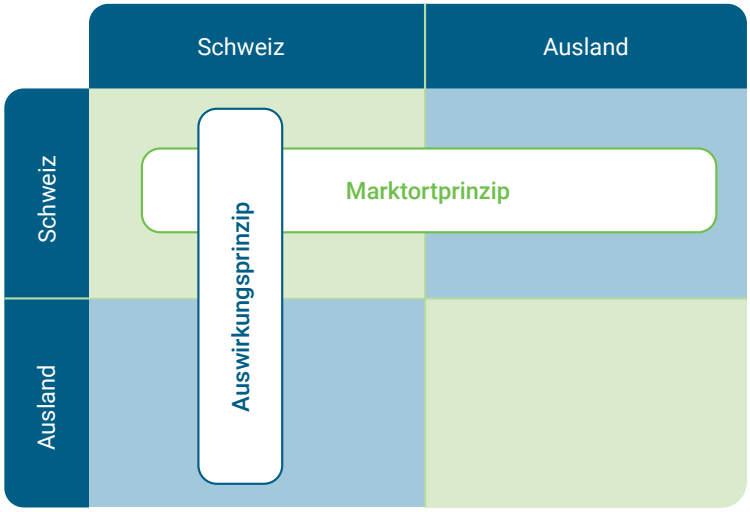
### 3. Inkrafttreten des neuen Datenschutzrechts

Das neue Datenschutzgesetz samt ergänzender Verordnungen wird am 01. September 2023 in Kraft treten. Zu beachten ist, dass es hierbei keine Übergangsfrist geben wird.

„Auswirkungsprinzip" beachten! Das revDSG sollte als Unternehmen mit dem geringsten Bezug zur Schweiz immer im Blick behalten werden.

Als Private im Sinne des revDSG sind auch Unternehmen zu verstehen, die über Daten natürlicher Personen verfügen. Die neuen Regelungen des revDSG sind folglich von allen Unternehmen (mit Sitz innerhalb oder ausserhalb der Schweiz) zu beachten, sobald sich die Datenbearbeitungen „in" der Schweiz auswirken (auch dann, wenn diese im Ausland veranlasst werden).

Ein besonders hohes Risiko, einen Verstoss zu begehen, besteht denklogischer Weise für Unternehmen, die mit grossen Mengen an Personendaten sowie besonders schützenswerten Daten regelmässig „hantieren", bspw. Onlineshops, Profiling, Krankenhäuser, etc.



## III. Die grössten Veränderungen zum bisherigen DSG

Das Schweizer Bundesgesetz über den Datenschutz wurde grundlegend revidiert. Doch was sind eigentlich die wesentlichen Änderungen?

1. **Neuer Geltungsbereich:** Die neuen Regelungen des revDSG sind nur auf Personendaten natürlicher Personen anzuwenden. Juristische Personen (also „Unternehmensdaten") werden nicht mehr erfasst.

2. **Erweiterter Umfang:** Grundsätzlich dürfen Personendaten in der Schweiz ohne Einwilligung bearbeitet werden. Eine Ausnahme gilt für „besonders schützenswerte Daten". Wie der Name schon sagt, muss hier das Schutzniveau etwas höher ausfallen und somit ist eine Einwilligung für das Bearbeiten dieser Daten erforderlich. Neu werden nun auch „genetische und biometrische Daten" vom Begriff der besonders schützenswerten Daten umfasst.

3. **Grundsätze „Privacy by Design"** (Datenschutz durch Technikgestaltung) und **"Privacy by Default"** (Datenschutz durch datenschutzfreundliche Voreinstellungen) werden eingeführt.

4. **Verbesserte Transparenz:** Eine der zentralsten Änderungen ist die neue Pflicht zur Erteilung gewisser Informationen über die Datenbearbeitung. Bereits bei Beschaffung von Personendaten müssen Betroffene informiert werden. Die wesentlichen Informationen / Inhalte sind im Art. 19 revDSG aufgelistet. Ein Blick ins Gesetz lohnt sich also. Und dann heißt es: Datenschutzerklärung für die Webseite erstellen, Datenschutzinformationen für Kund*innen, Bewerber*innen und Mitarbeiter*innen aufsetzen usw.

5. **Verzeichnis der Bearbeitungstätigkeiten:** Es wird obligatorisch. Der Verantwortliche muss nun ein Verzeichnis über sämtliche Bearbeitungstätigkeiten führen. Für Bundesbehörden dürfte das nichts Neues sein. Welche Inhalte in solch ein Verzeichnis gehören, steht in Art. 12 revDSG. Auch hier lohnt sich ein Blick ins neue Regelwerk. Und bevor Sie jetzt loslegen, sollten Sie erst prüfen, ob Sie überhaupt ein Verzeichnis der Bearbeitungstätigkeiten führen müssen. Denn die Datenschutzverordnung (DSV) sieht Ausnahmen vor! Aber Vorsicht: Nur weil Ihr Unternehmen weniger als 250 Mitarbeiter*innen beschäftigt, ist es nicht automatisch von der Pflicht befreit.

6. **Datenschutz-Folgenabschätzung:** Neu ist auch die Pflicht zum Erstellen einer Datenschutz-Folgenabschätzung, sofern die Datenbearbeitung ein hohes Risiko für die Persönlichkeit und die Grundrechte betroffener Personen mit sich bringt. Zunächst muss also erstmal eine Risikoanalyse stattfinden, ob überhaupt ein hohes Risiko besteht. Und denken Sie daran, dass Sie solch eine „aufwändige" Prüfung eigentlich bereits vor Einführung einer neuen Software oder Ähnlichem durchführen sollten.

7. **Profiling:** Auch der Begriff Profiling (die automatisierte Bearbeitung von Personendaten) ist neu und wurde in das revidierte Datenschutzgesetz aufgenommen. Wer sich bereits mit den Regelungen der DS-GVO beschäftigt hat, dürfte die Begrifflichkeit aber bereits schon kennen.

8. **Ausbau der Schweigepflicht zu einer allgemeinen Schweigepflicht für alle Berufstätigen:** Das Berufsgeheimnis im Datenschutzrecht wurde ausgebaut. Geheime Personendaten, die im Rahmen der Ausübung der beruflichen Tätigkeit anvertraut werden, müssen geheim gehalten werden. Wenn Sie deren Geheimhaltung nicht garantieren können, müssen Sie vorgängig klarstellen, mit wem Sie die Angaben möglicherweise teilen.

9. **Rechtsdurchsetzung und Sanktionen:** Das revDSG kann in einem öffentlich - rechtlichen Verfahren durch den EDÖB, in einem strafrechtlichen Verfahren durch die Staatsanwaltschaft bzw. Strafgerichte oder im Rahmen eines Klageverfahrens (keine Gerichtsgebühren) durch die Zivilgerichte durchgesetzt werden. Bei einem Vers-toss gegen das revDSG können grundsätzlich alle drei Verfahren angestrebt werden, wenn die Voraussetzungen dafür gegeben sind. Mit dem revDSG werden nun Bussen bis zu CHF 250,000 eingeführt. Achtung: Die Bussen werden nicht gegen Unternehmen verhängt, sondern gegen diejenige Privatperson, die im Unternehmen für die Datenbearbeitung zuständig ist. Eine direkte Sanktionierung des Unternehmens kommt nur dann in Frage, wenn die verantwortliche Person nicht ausfindig gemacht werden kann und wenn die Busse unter CHF 50,000 beträgt. Auch aus diesem Grund ist ein Schutz der Mitarbeiter*innen durch entsprechende technische Massnahmen unerlässlich.

10. **Rasche Meldung an den EDÖB:** Der EDÖB (Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter) übernimmt die Prüfung von Verletzungen der Datensicherheit und fungiert als Ansprechpartner in Fragen zur Umsetzung des revDSG. Es handelt sich hier um eine staatliche Stelle. Verletzungen der Datensicherheit (wie z.B. unbeabsichtigtes oder widerrechtliches Verlieren, Löschen, Vernichten oder Verändern von Personendaten) müssen dem EDÖB nun so rasch als möglich gemeldet werden, wenn sie voraussichtlich zu einem hohen Risiko für die Betroffenen führen. In der Regel muss der Verantwortliche auch die betroffene Person informieren, wenn dies zu ihrem Schutz nötig ist oder der EDÖB es verlangt. Eine starre Frist wie in der DS-GVO (72 Stunden) gibt das revDSG jedoch nicht vor.

Die Grundsätze sowie die Art und Weise der Datenbearbeitung sind allerdings gleichgeblieben.

Das Bearbeiten von Personendaten ist weiterhin ohne Einwilligung / ohne Rechtfertigungsgrund möglich.

## Was ist „Profiling“ und was ist „Profiling mit hohem Risiko“ laut revDSG?

**Art. 5 f) DSG**

**Profiling |** Jede Art der automatisierten Bearbeitung von Personendaten, die darin besteht, dass diese Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen

**Art. 5 g) DSG**

**Profiling mit hohem Risiko |** Profiling, das ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringt, indem es zu einer Verknüpfung von Daten führt, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt

# Das neue Schweizer...
# ...Datenschutzgesetz

**Sie brauchen Unterstützung in Sachen (Schweizer) Datenschutz und IT-Sicherheit?**

Dann ist die **MORGENSTERN IT & Privacy GmbH** genau das Richtige für Sie. Wir bieten eine Vielzahl an Leistungen rund um die Themen **Datenschutz und IT-Sicherheit**.

- **Basic Package**
- **Crossborder Package**
- **Advanced Package**
- **Crossborder Advanced Package**
- **Vertrag-Check Package**

morgenstern-privacy.ch


**» Jetzt Angebot anfordern**

**the future is yours.**

Unternehmen und Bundesbehörden sollten sich mit den neuen Regelungen des revDSG vertraut machen. Wichtig ist, dass die Ziele des Datenschutzes stets im Blick gehalten werden. Zwar mag das neue Datenschutzgesetz etwas mehr Bürokratieaufwand mit sich bringen, die Umsetzung der Regelungen ist jedoch kein „Hexenwerk". Und denken Sie daran, wenn Sie Fragen haben, wenden Sie sich gern an uns.

## IV. Regeln im Überblick | Betroffenenrechte

Das revDSG sieht verschiedene Pflichten für die datenbearbeitende Person vor, beispielsweise das Führen eines Verzeichnisses der Bearbeitungstätigkeiten gemäss Art. 12 revDSG, die Erteilung von Informationspflichten bei Beschaffung von Personendaten nach Art. 19 revDSG, die Einhaltung der Regelungen bei Bekanntgabe von Personendaten ins Ausland (Art. 16 – 18 revDSG) sowie die Durchführung einer Datenschutz-Folgenabschätzung nebst ggf. Meldung an den EDÖB (Art. 22 ff. revDSG).

Ausserdem müssen bei der Erfüllung dieser Anforderungen die Grundsätze der Datenbearbeitung aus Art. 6 revDSG immer beachtet werden.

Bei der Umsetzung dieser Anforderungen, die sich im Detail recht anspruchsvoll darstellt, sind wir von MORGENSTERN Ihnen gerne behilflich.

Besonders hervorzuheben sind die Betroffenenrechte in den Art. 25 ff. revDSG, die zwar im Vergleich zur DS-GVO reduziert geregelt sind, dadurch aber auch mehr Platz zur richterlichen Auslegung bieten:

**RECHT AUF BERICHTIGUNG UND VERGESSEN** INFORMATIONSPFLICHT
RECHT AUF LÖSCHUNG DER DATEN *WIDERSPRUCHSRECHT*

# Betroffenenrechte

*EINSCHRÄNKUNG DER DATEN* **RECHT AUF MENSCHLICHES GEHÖR**
RECHT AUF DATENHERAUSGABE AUSKUNFTSRECHT

- **Informationspflicht (Art. 19 revDSG)**
  Gemäss Art. 19 revDSG besteht eine angemessene Informationspflicht des Verantwortlichen über die Datenbearbeitung. Bekannt dürfte diese bereits aus der DS-GVO sein, die seit 2018 ebenfalls eine verbindliche Pflicht zur Bereitstellung gewisser Informationen an Betroffene regelt. Welche Inhalte in die „Datenschutzinformationen" gehören, ist im Gesetz geregelt. Art. 20 revDSG sieht daneben auch Ausnahmen vor, wann eine Informationspflicht entfällt bzw. entfallen könnte.

- **Recht auf menschliches Gehör im Falle einer automatisierten Einzelfallentscheidung (Art. 21 revDSG)**
  Sollte eine Person Objekt einer automatisierten Einzelfallentscheidung werden, muss sie entsprechend informiert werden und hat sodann Anspruch auf „menschliches Gehör".

- **Auskunftsrecht (Art. 25 revDSG)**
  Innerhalb von 30 Tagen muss die Auskunft schriftlich erteilt werden, wobei Art. 25 revDSG den Mindestumfang der mitzuteilenden Information festlegt. Kann die Auskunft nicht innert 30 Tagen seit dem Eingang des Begehrens erteilt werden, so muss der Verantwortliche die betroffene Person darüber in Kenntnis setzen. Aus diesem Grund ist es besonders wichtig, die Datenquellen richtig zu erfassen und insbesondere auch bei „Datenmigration" Genauigkeit walten zu lassen.

- **Widerspruchsrecht**, welches das **Recht auf Löschung der Daten/ Einschränkung der Daten** umfasst

- **Recht auf Datenherausgabe und -übertragung (Art. 28 revDSG)**

- **Recht auf Berichtigung und Vergessen (Art. 32 revDSG)**

Im Umgang mit Personendaten stellen sich im laufenden Geschäftsbetrieb immer wieder die Fragen, was man eigentlich darf und was nicht. Einige Beispiele:

- Wie darf nun im Rahmen des Marketings werbend an die Personen herangetreten werden?
- Dürfen Daten an Partnerunternehmen und Tochtergesellschaften weitergeben werden?
- Wie ist das mit dem Auftragsmanagement? Werden nun (neue) Verträge über die Auftragsbearbeitung benötigt?
- Wo unterscheiden sich revDSG und DS-GVO und was bedeutet das für die grenzübergreifende Datenbearbeitung?
- Besteht in der Schweiz auch ein Kopplungsverbot?

Für die Beantwortung dieser und ähnlicher Fragen müssen verschiedene gesetzliche Grundlagen berücksichtigt werden. Zum Beispiel auch das Bundesgesetz gegen den unlauteren Wettbewerb (UWG). Wir von MORGENSTERN unterstützen Sie gern bei Ihren Anliegen. Kontaktieren Sie uns einfach!

## V. Folgen der Verletzung der Datensicherheit

Als Unternehmen oder Bundesbehörde stellt sich die Frage, wie mit sogenannten „Data Breach Notifications" oder „Datenpannen" umgegangen werden muss und welche Strafen drohen.

Grundsätzlich kommen hier verschiedene Prüf- und Meldepflichten in Betracht. Selbstredend betreffen diese vor allem die betroffene Person, falls dies „zu ihrem Schutz" erforderlich ist. Es empfiehlt sich, bereits interne Notfallpläne / Kommunikations- und Informationskonzepte vorbereitet zu haben, um im Fall der Fälle kurzfristig reagieren zu können. Mit dem richtigen Workflow und regelmässigen Schulungen und Sensibilisierungsmassnahmen für Mitarbeiter*innen kann das Risiko einer Verletzung der Datensicherheit (und somit auch dem Datenschutz) eingedämmt werden.

**Wir von MORGENSTERN assistieren hierbei gern!**

Darüber hinaus kommt eventuell eine Meldung an den EDÖB in Betracht, die „so rasch wie möglich" stattfinden muss. Diese Kontaktaufnahme kann in Einzelfällen umgangen werden, indem stattdessen ein*e **Datenschutzberater*in** bestellt wird. Dies hat den Vorteil, dass nicht direkt eine offizielle Stelle über Interna Auskunft erhält.

Auch hierzu informieren wir gern vertiefend. Die Ernennung eines/ einer Datenschutzberater*in kann durchaus Sinn machen, wobei dieser auch „von extern" kommen darf.

MORGENSTERN

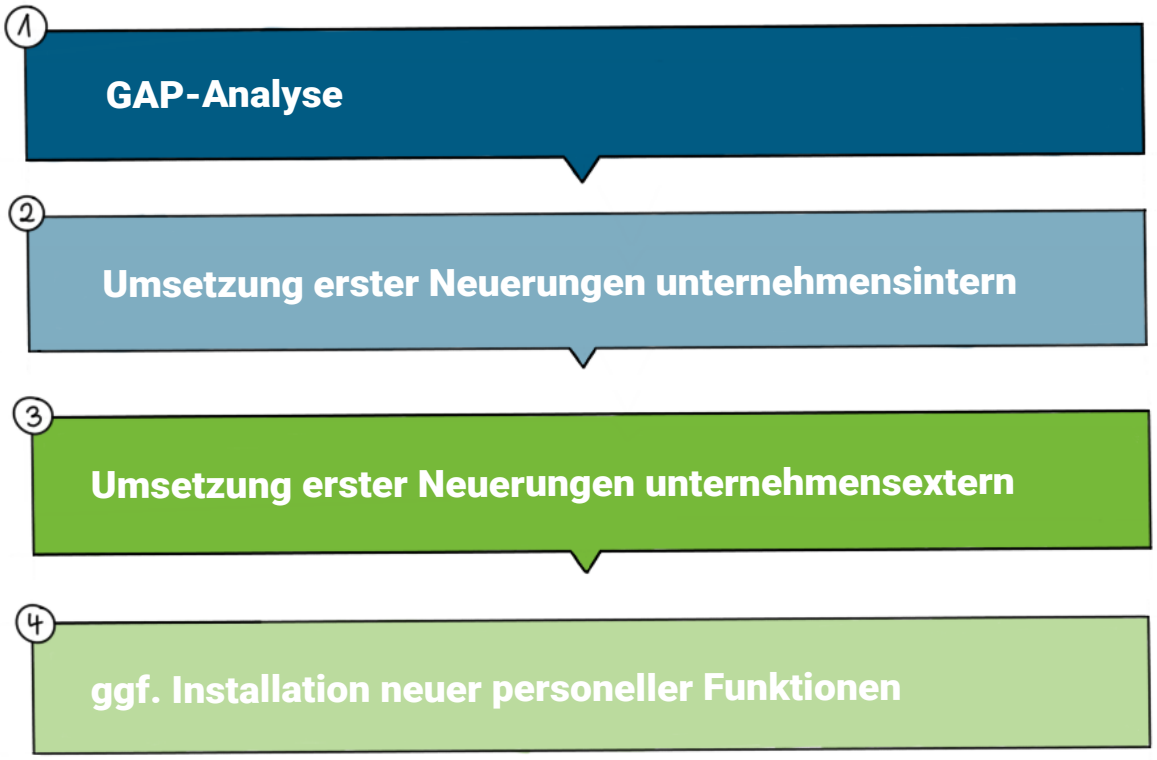
## 1. Sanktionen

Wie bereits dargelegt, werden im revDSG Bussen bis zu CHF 250`000 angedroht. Sich gegen solche Bussen bei einer Versicherung versichern zu lassen, ist wohl nicht möglich.

Nicht zu vernachlässigen ist jedoch auch der Aspekt der „schlechten Presse", den eine solche Pflichtverletzung nach sich zieht und der damit einhergehenden ökonomischen Verluste.

Selbstredend wird die Veränderung des revDSG jedes Unternehmen in der Schweiz vor Herausforderungen stellen und Transformationen nötig machen. Wie weitgehend und drängend diese sind hängt davon ab, welche Datenbearbeitungsprozesse der Geschäftsbetrieb konkret für seine Arbeit benötigt und inwieweit er sich bereits DS-GVO-konform angepasst hat.

Um Schweizer Unternehmen in ihrem Ziel, revDSG-konform zu arbeiten, wettbewerbsfähig zu halten und zur unkomplizierten Datenbearbeitung zu führen, sollten die folgenden Schritte befolgt werden:



**1. GAP-Analyse**
Analyse des Ist-Standes: Welche Datenbearbeitung ist für die Unternehmenstätigkeit unerlässlich? Wo besteht datenschutzrechtlicher Handlungsbedarf?

**2. Umsetzung erster Neuerungen unternehmensintern**
Erstellen und Anpassen interner Richtlinien zur Datenbearbeitung sowie internes Implementieren angepasster Prozesse, bspw. Handling von Betroffenenanfragen, Meldung von Datenschutzverletzungen, Durchführung von Datenschutz-Folgenabschätzung, Erstellung und Implementierung von technischen und organisatorischen Massnahmen (TOM), Erstellung eines Verzeichnisses der Bearbeitungstätigkeiten, Sensibilisierung der Mitarbeiter *innen durch Schulungen etc.

**3. Umsetzung erster Neuerungen unternehmensextern**
Bspw. Überprüfen und Anpassen der Verträge mit Auftragsbearbeitern(Dritten), Anpassung von Datenschutz-Setup und Datenschutzerklärung, Überprüfung bestehender Verträge

**4. ggf. Installation neuer personeller Funktionen**
Bspw. Datenschutzberater*in, Vertreter*in in EU / CH

## BERATUNG DURCH MORGENSTERN

Aufgrund der umfassenden Erfahrung von MORGENSTERN in sämtlichen Bereichen des Datenschutzes und im IT-Sektor können wir Sie bei allen Themen rund um Digitalisierung, Datenspeicherung, Datensicherung und Datenverwendung auch grenzübergreifend optimal unterstützen.

Sei es bei alltäglichen Fragen der Datennutzung, der Anpassung Ihres CRM-Systems, Herausforderungen aus dem Marketing-Bereich, Speicherung und Weitergabe von Daten oder der Expansion Ihres Unternehmens (evtl. auch über die Landesgrenzen hinaus) - wir bei MORGENSTERN beraten Sie gern.


**MORGENSTERN IT & Privacy GmbH**

Churerstrasse 54
CH - 8808 Pfäffikon SZ

**Telefon**
+41 55 415 70 70

**E-Mail**
contact@morgenstern-privacy.ch