

FSDZ Rechtsanwälte &  
Notariat AG

**konova**

# Revidiertes Datenschutzgesetz

Auswirkungen auf den digitalen Bürgerdialog

# Agenda

- Revidiertes Datenschutzgesetz
- Digitaler Bürgerdialog
- Auswirkungen auf den Datenschutz
- Umsetzung in der Praxis
- Fragen und Antworten

# Vorstellung

**konova**



E-Mitwirkung



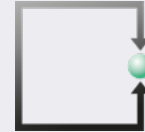
**Miro Hegnauer**

Partner, CEO

Dipl. Wirtschaftsinformatiker

[hegnauer@konova.ch](mailto:hegnauer@konova.ch)

[www.konova.ch](http://www.konova.ch)



**FSDZ Rechtsanwälte &  
Notariat AG**



**Milica Stefanovic**

Rechtsanwältin

MLaw

[stefanovic@fsdz.ch](mailto:stefanovic@fsdz.ch)

[www.fsdz.ch](http://www.fsdz.ch)

# **Revidiertes Datenschutzgesetz**

# Einführung revidiertes Datenschutzgesetz

## Übersicht

1. Einführung neues Datenschutzgesetz
2. Anwendung neues Datenschutzgesetz
  - Persönlicher und sachlicher Geltungsbereich
  - Geltungsbereich Bund – Kantone – Private
3. Anwendung kantonales Datenschutzgesetz (Beispiel Kanton Bern)
4. Wichtigste Neuerungen im neuen Datenschutzgesetz
5. Grundsätze nach nDSG

# Anwendung neues Datenschutzgesetz



Das neue Datenschutzgesetz (nDSG) und die neue Datenschutzverordnung (DSV) sowie die neue Verordnung über Datenschutzzertifizierungen (VDSZ) treten am 1. September 2023 in Kraft. Mit der Totalrevision wird das DSG den veränderten technologischen und gesellschaftlichen Verhältnissen angepasst. Dabei werden insbesondere die Transparenz von Datenbearbeitungen verbessert und die Selbstbestimmung der betroffenen Personen über ihre Daten gestärkt.

## - 8. Kapitel: Strafbestimmungen

### - Art. 60 Verletzung von Informations-, Auskunfts- und Mitwirkungspflichten

<sup>1</sup> Mit Busse bis zu 250 000 Franken werden private Personen auf Antrag bestraft:

- a. die ihre Pflichten nach den Artikeln 19, 21 und 25–27 verletzen, indem sie vorsätzlich eine falsche oder unvollständige Auskunft erteilen;
- b. die es vorsätzlich unterlassen:
  1. die betroffene Person nach den Artikeln 19 Absatz 1 und 21 Absatz 1 zu informieren, oder
  2. ihr die Angaben nach Artikel 19 Absatz 2 zu liefern.

<sup>2</sup> Mit Busse bis zu 250 000 Franken werden private Personen bestraft, die unter Verstoß gegen Artikel 49 Absatz 3 dem EDÖB im Rahmen einer Untersuchung vorsätzlich falsche Auskünfte erteilen oder vorsätzlich die Mitwirkung verweigern.

Wer gegen die Datenschutzvorschriften verstösst, kann künftig mit einer Busse von bis zu CHF 250'000.00 bestraft werden.

# Anwendung neues Datenschutzgesetz

## Persönlicher und sachlicher Geltungsbereich

### Art. 2 Persönlicher und sachlicher Geltungsbereich

<sup>1</sup> Dieses Gesetz gilt für die Bearbeitung von Personendaten natürlicher Personen durch:

a. private Personen;

b. Bundesorgane.

Streichung: Schutz der Daten juristischer Personen

natürlicher Personen

Unternehmen sind auch private Personen

Kantone erlassen 26 Kantons-DSG

<sup>2</sup> Es ist nicht anwendbar auf:

- a. Personendaten, die von einer natürlichen Person ausschliesslich zum persönlichen Gebrauch bearbeitet werden;
- b. Personendaten, die von den eidgenössischen Räten und den parlamentarischen Kommissionen im Rahmen ihrer Beratungen bearbeitet werden;

# Anwendung neues Datenschutzgesetz

## Geltungsbereich Bund – Kantone - Private

### CH-DSG gilt für


- Bundesbehörden und
- Private (natürliche Personen und Unternehmen)




Kantone erlassen jetzt laufend ihre 26 (!! ) neuen kantonalen DSG für ihre

- kantonalen Verwaltungen, ihre eigenen öffentlich-rechtlichen Körperschaften (z.B. Spitäler, Gebäudeversicherung, Informatikbetriebe, EW etc.) und
- die Gemeinden.






# Wer ist zuständig?

Kanton St.Gallen 

## Datenschutz in den Gemeinden

Für die Einhaltung des kantonalen Datenschutzrechts auf Gemeindeebenen sind die Gemeindefachstellen zuständig. Betrifft Ihr Anliegen die Bearbeitung von Personendaten im Zusammenhang mit einer Behörde der Gemeindeverwaltung, ist die entsprechende Gemeindefachstelle zuständig.

  Vorlesen 

Das Datenschutzgesetz des Kantons St.Gallen gewährt Ihnen auf kantonaler und kommunaler Ebene die gleichen Rechte. Mehr über diese Rechte, erfahren Sie in der Rubrik "[Kantonaler Datenschutz](#)".

Die Fachstellen für Datenschutz der Gemeinden überprüfen auf Anzeige betroffener Personen die Einhaltung der Datenschutzbestimmungen durch die öffentlichen Organe der Gemeinden.

Die Gemeinden müssen eigene Datenschutzfachstellen einrichten. Etliche Gemeinden haben sich in den regionalen Gemeindefachstellen zusammengeschlossen. Die Gemeinden Flawil und St. Gallen führen eine eigene Fachstelle. Die Anschrift Ihrer Gemeindefachstelle finden Sie "[hier](#)".

Quelle: <https://www.sg.ch/sicherheit/datenschutz/meine-rechte/datenschutz-in-den-gemeinden.html>

«Der Datenschutzbeauftragte (DSB) hat als unabhängige Aufsichtsstelle die Einhaltung der Vorschriften über den Datenschutz in der **kantonalen und kommunalen Verwaltung zu überwachen. Er berät die Verwaltungsstellen in allen datenschutzrechtlichen Belangen, sorgt für deren **Ausbildung und bearbeitet Anfragen und Gesuche von auskunftersuchenden Personen.****»

# Anwendung neues Datenschutzgesetz Kantonales Datenschutzgesetz (Kanton Bern)

## **Art. 4** Geltungsbereich

<sup>1</sup> Dieses Gesetz gilt für jedes Bearbeiten von Personendaten durch Behörden.

<sup>2</sup> Es findet keine Anwendung,

- a wenn eine Behörde mit privaten Personen im wirtschaftlichen Wettbewerb steht und nicht hoheitlich handelt. Die Aufsicht richtet sich jedoch nach den Artikeln 32–37;
- b wenn ein Mitarbeiter einer Behörde Personendaten zu ausschliesslich persönlichem Gebrauch bearbeitet, namentlich um über ein persönliches Arbeitsmittel zu verfügen;
- c \* auf hängige Verfahren der Zivil- oder Strafrechtspflege, auf hängige Verfahren der Verwaltungsrechtspflege mit Ausnahme der Verwaltungsverfahren sowie auf Ermittlungen einer parlamentarischen Untersuchungskommission.

# Wichtigste Neuerungen im neuen Datenschutzgesetz

1. Nur noch Daten natürlicher Personen sind künftig betroffen.
2. Genetische und biometrische Daten werden in die Definition der besonders schützenswerten Personendaten aufgenommen.
3. Grundsätze „Privacy by Design“ und „Privacy by Default“
4. Datenschutz-Folgenabschätzung
5. Informationspflicht ausgeweitet
6. Verzeichnis der Bearbeitungstätigkeiten
7. Meldepflicht
8. Begriff Profiling

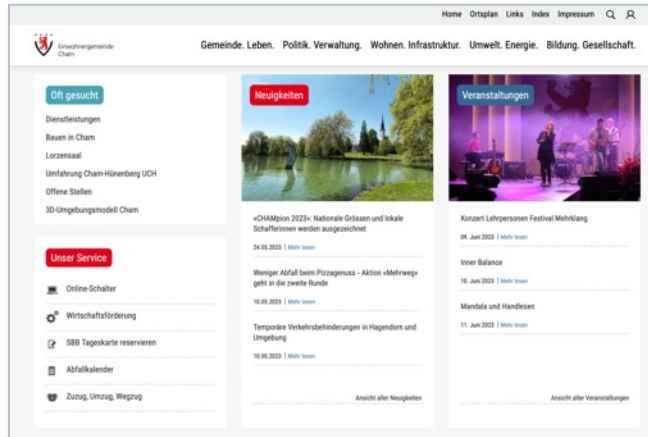
# Grundsätze nach nDSG

## - Art. 6 Grundsätze

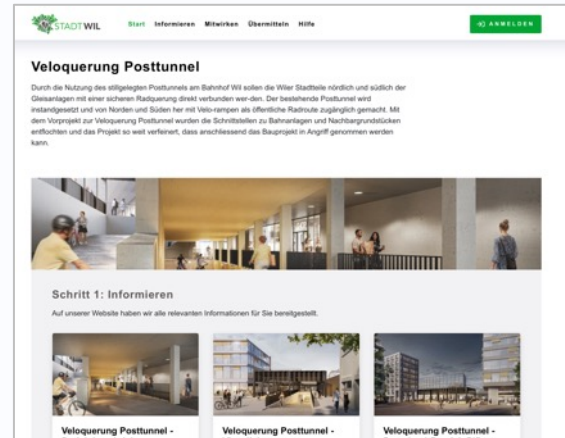
- <sup>1</sup> Personendaten müssen rechtmässig bearbeitet werden.
- <sup>2</sup> Die Bearbeitung muss nach Treu und Glauben erfolgen und verhältnismässig sein.
- <sup>3</sup> Personendaten dürfen nur zu einem bestimmten und für die betroffene Person erkennbaren Zweck beschafft werden; sie dürfen nur so bearbeitet werden, dass es mit diesem Zweck vereinbar ist.
- <sup>4</sup> Sie werden vernichtet oder anonymisiert, sobald sie zum Zweck der Bearbeitung nicht mehr erforderlich sind.
- <sup>5</sup> Wer Personendaten bearbeitet, muss sich über deren Richtigkeit vergewissern. Sie oder er muss alle angemessenen Massnahmen treffen, damit die Daten berichtigt, gelöscht oder vernichtet werden, die im Hinblick auf den Zweck ihrer Beschaffung oder Bearbeitung unrichtig oder unvollständig sind. Die Angemessenheit der Massnahmen hängt namentlich ab von der Art und dem Umfang der Bearbeitung sowie vom Risiko, das die Bearbeitung für die Persönlichkeit oder Grundrechte der betroffenen Personen mit sich bringt.
- <sup>6</sup> Ist die Einwilligung der betroffenen Person erforderlich, so ist diese Einwilligung nur gültig, wenn sie für eine oder mehrere bestimmte Bearbeitungen nach angemessener Information freiwillig erteilt wird.
- <sup>7</sup> Die Einwilligung muss ausdrücklich erfolgen für:
  - a. die Bearbeitung von besonders schützenswerten Personendaten;
  - b. ein Profiling mit hohem Risiko durch eine private Person; oder
  - c. ein Profiling durch ein Bundesorgan.

# **Digitaler Bürgerdialog und Datenschutz**

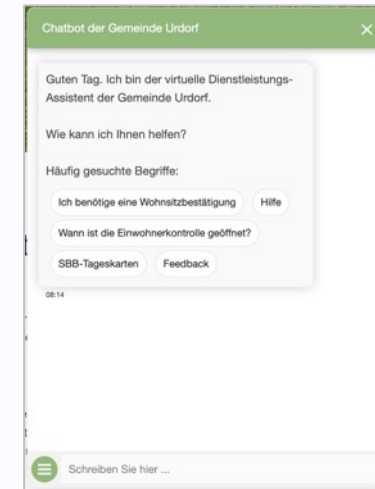
# Digitaler Bürgerdialog



Gemeindewebsite



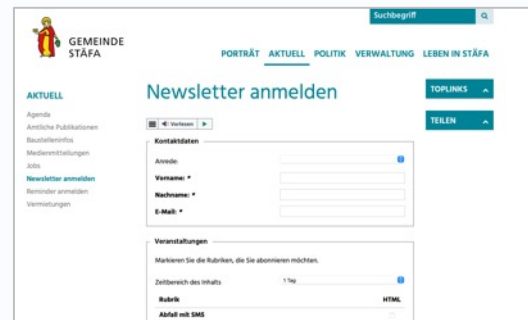
E-Mitwirkung



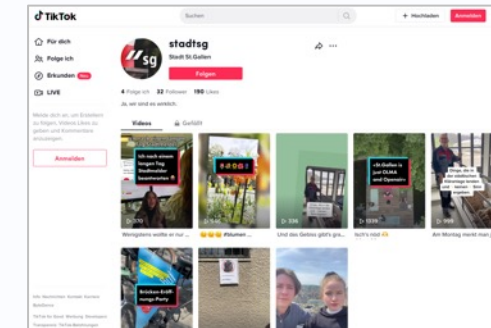
Chatbot



Digitaler Dorfplatz



Newsletter



Social Media

# Auswirkungen auf den Datenschutz

Weshalb, welche und wie  
werden personenbezogene  
Daten verarbeitet?

# Weshalb: Rechtliche Grundlagen zur Verarbeitung von personenbezogenen Daten

## Art. 5 Zulässigkeit a allgemein

- 1 Personendaten dürfen nur bearbeitet werden, wenn das Gesetz ausdrücklich dazu ermächtigt oder wenn das Bearbeiten der Erfüllung einer gesetzlichen Aufgabe dient.
- 2 Der Zweck des Bearbeitens muss bestimmt sein.
- 3 Die Personendaten und die Art des Bearbeitens müssen für die Aufgabenerfüllung geeignet und notwendig sein.

*Datenschutzgesetz Kanton Bern*

### Beispiel:



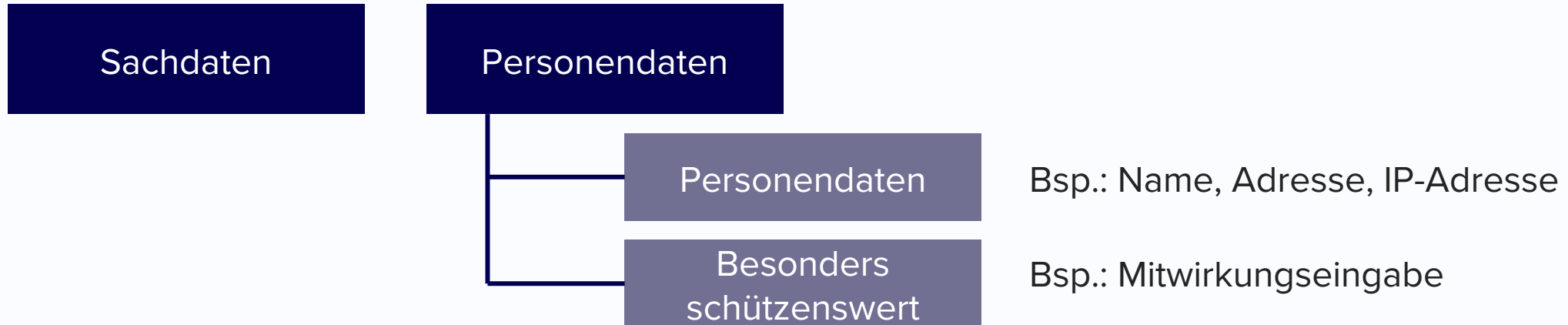
E-Mitwirkung

## § 6 \* Information und Mitwirkung der Bevölkerung

- 1 Der Kanton, die regionalen Entwicklungsträger und die Gemeinden unterrichten die Bevölkerung und weitere Betroffene frühzeitig über die Ziele und Inhalte ihrer Planungen und Konzepte nach diesem Gesetz.
- 2 Sie sorgen dafür, dass die Bevölkerung und weitere Betroffene in geeigneter Weise mitwirken können.



# Welche: Klassifizierung von Daten



## Art. 3 Besonders schützenswerte Personendaten

<sup>1</sup> Besonders schützenswerte Personendaten sind Angaben über

- a die religiöse, weltanschauliche oder politische Ansicht, Zugehörigkeit und Betätigung sowie die Rassenzugehörigkeit;
- b den persönlichen Geheimbereich, insbesondere den seelischen, geistigen oder körperlichen Zustand;
- c Massnahmen der sozialen Hilfe oder fürsorgerischen Betreuung;
- d polizeiliche Ermittlungen, Strafverfahren, Straftaten und die dafür verhängten Strafen oder Massnahmen.

Datenschutzgesetz Kanton Bern

# Wie: Verarbeitung von Daten

## Einwilligungspflicht

**Art. 6** b besonders schützenswerte Personendaten

<sup>1</sup> Besonders schützenswerte Personendaten dürfen nur bearbeitet werden, wenn zusätzlich

- a die Zulässigkeit sich aus einer gesetzlichen Grundlage klar ergibt, oder
- b die Erfüllung einer gesetzlichen Aufgabe es zwingend erfordert, oder
- c die betroffene Person ausdrücklich zugestimmt hat.

*Datenschutzgesetz Kanton Bern*

## Schutz der Daten

§ 7. <sup>1</sup> Das öffentliche Organ schützt Informationen durch angemessene organisatorische und technische Massnahmen. Informations-sicherheit

*Datenschutzgesetz Kanton Zürich*

# Rechte der Bürgerinnen und Bürger

## 4 Rechte der betroffenen Person

### Art. 20 Einsicht in das Register

<sup>1</sup> Jede Person kann in das Register der Datensammlungen Einsicht nehmen.

### Art. 21 Auskunft a Grundsatz

<sup>1</sup> Jede Person kann von der verantwortlichen Behörde Auskunft verlangen, welche Daten über sie in einer Datensammlung bearbeitet werden. Sie hat sich über ihre Identität auszuweisen.

<sup>2</sup> Auf dieses Recht kann nicht zum voraus verzichtet werden.

<sup>3</sup> Die Auskunft wird in allgemeinverständlicher Form und auf Verlangen schriftlich erteilt.

<sup>4</sup> Die betroffene Person erhält auf Verlangen Einsicht in ihre Daten, wenn nicht wichtige und überwiegende öffentliche Interessen oder besonders schützenswerte Interessen Dritter entgegenstehen.

### Art. 22 b Einschränkungen

<sup>1</sup> Die Auskunft kann soweit verweigert oder aufgeschoben werden, als ein Gesetz dies verlangt oder besonders schützenswerte Interessen Dritter es erfordern.

<sup>2</sup> Kann die Auskunft dem Gesuchsteller selber nicht erteilt werden, weil sie ihn zu stark belasten würde, so kann sie einer Person seines Vertrauens gegeben werden.

### Art. 23 Berichtigung

<sup>1</sup> Jede Person hat Anspruch darauf, dass unrichtige oder nicht notwendige Personendaten über sie berichtigt oder vernichtet werden.

<sup>2</sup> Bestreitet die verantwortliche Behörde die Unrichtigkeit, so hat sie die Richtigkeit der Personendaten zu beweisen. Die betroffene Person hat im Rahmen des Zumutbaren bei der Abklärung mitzuwirken.

<sup>3</sup> Kann weder die Richtigkeit noch die Unrichtigkeit von Personendaten, insbesondere von solchen, die eine Wertung menschlichen Verhaltens enthalten, bewiesen werden, so kann die betroffene Person verlangen, dass eine angemessene Gegendarstellung aufgenommen wird.

### Art. 24 Andere Ansprüche

<sup>1</sup> Jede Person hat Anspruch darauf, dass Personendaten, die widerrechtlich bearbeitet worden sind, vernichtet oder sonst die Folgen der Widerrechtlichkeit beseitigt werden.

<sup>2</sup> Weist die betroffene Person ein schützenswertes Interesse nach, so ist der Entscheid den von ihr bezeichneten Behörden und Dritten bekanntzugeben.

### Art. 25 Haftung

<sup>1</sup> Für den Schaden, den ihre Behörden, Organe, Angestellten und Beauftragten durch widerrechtliches Bearbeiten von Personendaten den betroffenen Personen zufügen, haften \*

a \* der Kanton,

b \* die Gemeinden,

c \* Körperschaften, Anstalten und Private, soweit ihnen öffentliche Aufgaben übertragen sind,

d \* die Landeskirchen und ihre regionalen Einheiten.

<sup>2</sup> Sofern es die Schwere der Verletzung rechtfertigt und diese nicht anders wieder gutgemacht werden kann, so besteht Anspruch auf Genugtuung.

<sup>3</sup> Wurde der Schaden vorsätzlich oder grobfahrlässig verursacht, steht dem Ersatzpflichtigen der Rückgriff zu.

*Datenschutzgesetz Kanton Bern*

*Datenschutzgesetz Kanton Bern*

# Datenschutz und Datensicherheit

§ 7. <sup>1</sup> Das öffentliche Organ schützt Informationen durch angemessene organisatorische und technische Massnahmen. Informationssicherheit

<sup>2</sup> Die Massnahmen richten sich nach den folgenden Schutzzielen:

- a. Informationen dürfen nicht unrechtmässig zur Kenntnis gelangen,
- b. Informationen müssen richtig und vollständig sein,
- c. Informationen müssen bei Bedarf vorhanden sein,
- d. Informationsbearbeitungen müssen einer Person zugerechnet werden können,
- e. Veränderungen von Informationen müssen erkennbar und nachvollziehbar sein.

<sup>3</sup> Die zu treffenden Massnahmen richten sich nach der Art der Information, nach Art und Zweck der Verwendung und nach dem jeweiligen Stand der Technik.

Datenschutzgesetz Kanton Zürich

# Umsetzung in der Praxis

# Bürgerdialog etablieren



## Selber betreiben

- Betrieb der Lösung im eigenen Rechenzentrum
- Kein Zugriff des Softwareanbieters
- Verwaltung ist selbständig für die Einhaltung und Umsetzung der technischen und organisatorischen Massnahmen verantwortlich
- Meistens hohe Aufwände und Kosten für die Wartung

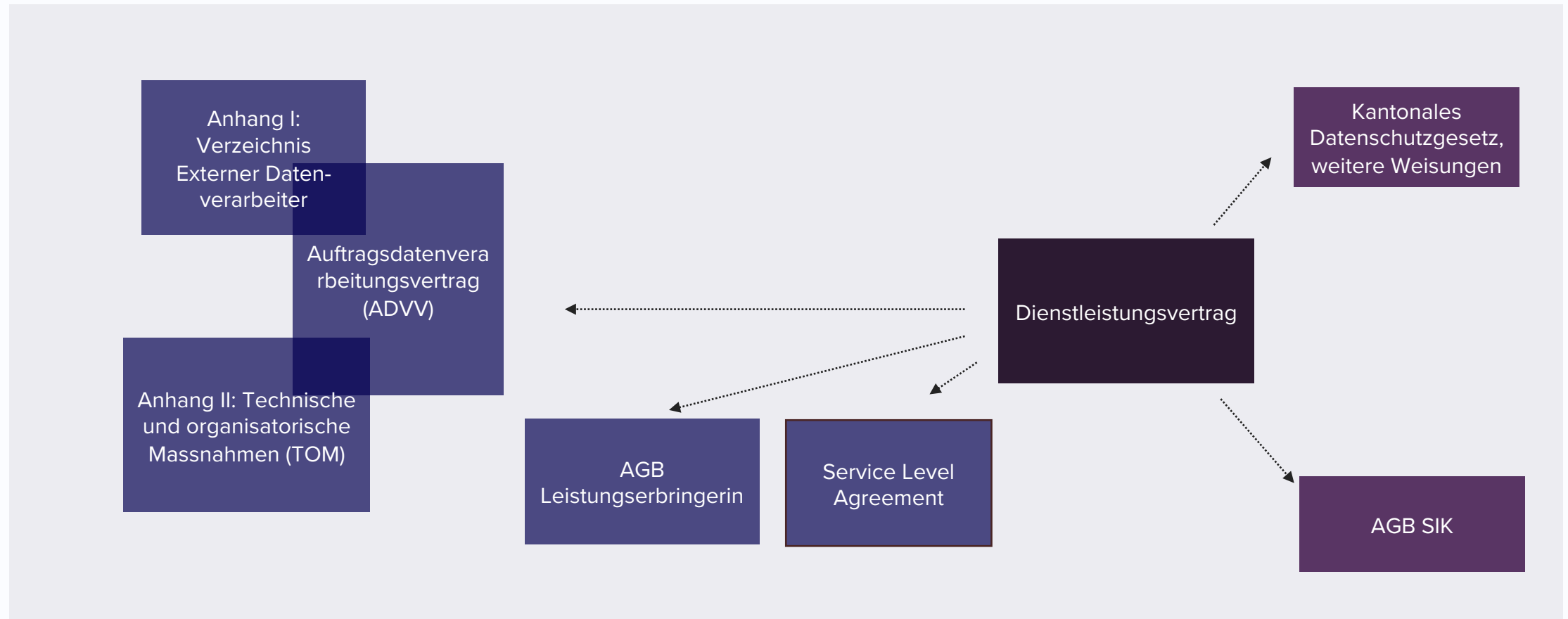


## Cloud / SaaS

- Betrieb der Lösung durch einen Drittanbieter
- Zugriff des Softwareanbieters auf die Daten
- Verwaltung beauftragt den Anbieter für die Einhaltung und Umsetzung der technischen und organisatorischen Massnahmen
- Geringere Kosten und Aufwände dank Unterstützung Standardisierung und Professionalisierung

# Sauberes Vertragswerk ausarbeiten

Die Verwaltung muss sicherstellen, dass der Drittanbieter die gleichen oder höheren Schutzmassnahmen umsetzt.



# Dienstleistungsvertrag

## - Art. 9 Bearbeitung durch Auftragsbearbeiter

<sup>1</sup> Die Bearbeitung von Personendaten kann vertraglich oder durch die Gesetzgebung einem Auftragsbearbeiter übertragen werden, wenn:

- a. die Daten so bearbeitet werden, wie der Verantwortliche selbst es tun dürfte; und
- b. keine gesetzliche oder vertragliche Geheimhaltungspflicht die Übertragung verbietet.

<sup>2</sup> Der Verantwortliche muss sich insbesondere vergewissern, dass der Auftragsbearbeiter in der Lage ist, die Datensicherheit zu gewährleisten.

<sup>3</sup> Der Auftragsbearbeiter darf die Bearbeitung nur mit vorgängiger Genehmigung des Verantwortlichen einem Dritten übertragen.

<sup>4</sup> Er kann dieselben Rechtfertigungsgründe geltend machen wie der Verantwortliche.

- Leistungen (Lizenz, Wartung, Support, Einführung)
- Konditionen
- Zusammenarbeit (Mitwirkung des Kunden, Projektorganisation)
- Haftung
- Datenschutz (Verweis auf ADVV und kantonales Datenschutzgesetz)
- Evtl. Verweis auf Service Level Agreement (SLA)



# Auftragsdatenverarbeitungsvertrag (ADV) (ADV)

Wie geht der Drittanbieter mit personenbezogenen Daten um?

## Inhalte:

- Ort der Datenverarbeitung
- Art und Kategorien der Personendaten
- Pflichten
- Technische und organisatorische Massnahmen
- Unterauftragsverhältnisse
- Kopien, Löschung und Rückgabe der Daten

**Technische und organisatorische Massnahmen**

	<input checked="" type="checkbox"/> Schliesssystem
Zugangskontrolle (Keine unbefugte Systembenutzung)	<input checked="" type="checkbox"/> (sichere) Kennwörter <input checked="" type="checkbox"/> Zwei-Faktor-Authentifizierung <input checked="" type="checkbox"/> Automatische Sperrung (z.B. Kennwort oder Pausenschaltung) <input checked="" type="checkbox"/> Zuordnung von Benutzerrechten

**Verzeichnis externer Datenverarbeiter**

2. Flowmailer B.V.

Flowmailer ist ein API-basierter Service zum Versand von transaktionalen E-Mails. Die Nutzung des Service im Rahmen der E-Mitwirkung erfolgt im Interesse des sicheren Versands und der verifizierten Zustellung von automatisierten E-Mail-Bestätigungen und E-Mail-Benachrichtigungen.

Firmensitz: Flowmailer B.V., Van Nelleweg 1, 3044 Rotterdam, Niederlande

Ort der Datenverarbeitung: Region Amsterdam, Niederlande (EU)

Verarbeitungszweck:

- Versenden von applikations-relevanten E-Mails
- Nachvollziehbarkeit der Zustellung bei Supportanfragen

Datenkategorien:

- Personendaten
  - E-Mail-Adresse
  - Anrede
  - Vorname
  - Nachname
- Sachdaten

Kategorie betroffener Personen:

- Beschäftigte
- Kunden

Löschfrist: 30 Tage

Periodizität: Dauernd

ADV abgeschlossen:  ja  nein

Zertifizierungen: ISO27001

Bemerkung:

- Die Rechenzentren werden von den Firmen Digital Realty, Schuberg Philis, and Iron Mountain betrieben. Die Hardware und Infrastruktur ist vollständig im Eigentum der Flowmailer B.V.
- Als Alternative kann der Kunde den eigenen SMTP-Server anbinden, sofern dieser öffentlich zugänglich ist.

Weitere Informationen: <https://flowmailer.com/en/resources/all?tab=legal>

# Datenschutzbestimmungen

*Erläuterungen gegenüber den Nutzenden, wie die Daten verarbeitet werden.*

## Inhalte:

- Wer ist verantwortlich?
- Was ist der Zweck, die rechtliche Grundlage?
- Welche Daten werden wie verarbeitet?
- Rechte der Nutzerinnen und Nutzer

## Datenschutz- und Nutzungsbestimmungen zur Web-Applikation E-Mitwirkung

Version 2.0, gültig ab dem 1. Juni 2023

Mit diesen Datenschutz- und Nutzungsbestimmungen möchte die verantwortliche Behörde (nachfolgend: «Verantwortliche» genannt) darüber informieren, welche Personendaten im Zusammenhang mit der Nutzung der Web-Applikation «E-Mitwirkung» (nachfolgend: «Web-Applikation» genannt) erhoben und bearbeitet werden, für welche Zwecke diese Personendaten genutzt werden und an wen sie allenfalls weitergegeben werden.

Ferner werden die betroffenen Personen (nachfolgend «Betroffene» genannt) mit diesen Datenschutz- und Nutzungsbestimmungen über die ihnen zustehenden Rechte aufgeklärt. Die Datenschutz- und Nutzungsbestimmungen gelten unabhängig der verwendeten Domains, Betriebssysteme, Plattformen und Geräte (z.B. Desktop oder Mobile), auf denen das Onlineangebot ausgeführt wird.

### 1. Verantwortliche

Die Verantwortliche für die Web-Applikation ist dem Impressum, verlinkt in der Fusszeile der Applikation, zu entnehmen.

### 2. Allgemeines zur Web-Applikation E-Mitwirkung

2.1 Die Web-Applikation dient der elektronischen Beteiligung von natürlichen Personen (in der Regel die Einwohner/Innen) sowie den interessierten Organisationen (nachfolgend: «Nutzer» genannt) an der Meinungsbildung sowie der Entscheidungsfindung im Rahmen der Zuständigkeiten des Verantwortlichen. Die elektronische Beteiligung zum jeweiligen Geschäft trägt zu einer niederschweligen Partizipation sowie einer effizienten Auswertung der Stellungnahmen der Betroffenen und den teilnehmenden Organisationen bei und verbessert dadurch die Qualität der Gesetzgebung, der Strategieerarbeitung und der Verwaltungsarbeit der Verantwortlichen.

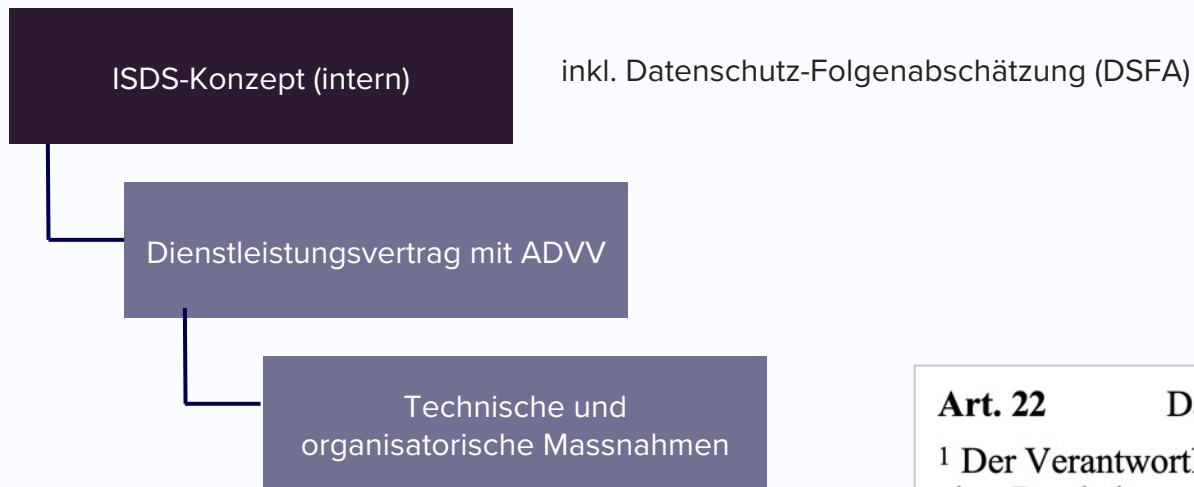
2.2 Der Begriff «Nutzer» umfasst alle Kategorien der die Web-Applikation einsetzenden natürlichen Personen, selbst wenn diese im Namen und Auftrag einer Organisation, Körperschaft, politischen Partei oder Unternehmung arbeiten. Der Begriff «Nutzer» wird zudem geschlechtsneutral verstanden. Als Nutzer können auch teilnehmende Organisationen in Frage kommen. Die nachfolgenden Bestimmungen beziehen sich auch auf deren Informationsbereitstellung zugunsten der Verantwortlichen.

2.3. Im Rahmen der Web-Applikation werden formelle und informelle Beteiligungen unterschieden. Abhängig davon, ob es sich um eine formelle Beteiligung (Ziffer 3.2.) handelt, werden die erfassten Rückmeldungen zur späteren Übermittlung an die Verantwortliche gespeichert (formell) oder direkt für andere Nutzer in der Applikation veröffentlicht (informell).

# ISDS-Konzept

«Das Informationssicherheit und Datenschutz-Konzept bildet die Grundlage für die **Festlegung der Massnahmen** für die **Informationssicherheit** und den **Datenschutz**. Es zeigt die **Restrisiken** auf, die mit dem Betrieb des **IT-Systems** und der **Organisation** verbunden sind. Es beschreibt das **Notfallkonzept**.»

HERMES, <https://www.hermes.admin.ch>



## 8 Risikoanalyse und Schutzmassnahmen

Im Rahmen der durchgeführten Risikoanalyse wurden die verschiedenen Risiken in den Kategorien Verfügbarkeit, Vertraulichkeit, Integrität und Nachvollziehbarkeit anhand der Eintrittswahrscheinlichkeit und den Auswirkungen bewertet. Das folgende Kapitel gibt einen Überblick über die Erkenntnisse der Risikoanalyse. Die Details sind der Excel-Datei zu entnehmen.

### 8.1 Resultate Risikoanalyse

Die Risiko-Analyse zeigt auf, dass die meisten Risiken als tief bewertet werden können. Dies, da die Leistungserbringerin bereits zahlreiche organisatorische und technische Massnahmen getroffen hat, um bekannte Risiken zu minimieren. Folgende vier Risiken wurden mit der Einstufung «gelb» markiert.

Nr.	Risiko
R6	Fehlplanung oder fehlende Anpassung, Ressourcenmangel
R7	Softwareschwachstelle oder -Fehler
R11	Unberechtigte oder fehlerhafte Nutzung oder Administration von Geräten und Systemen, Missbrauch von Berechtigungen
R18	Die Identität der Mitwirkungsteilnehmenden kann nicht vollständig sichergestellt werden.

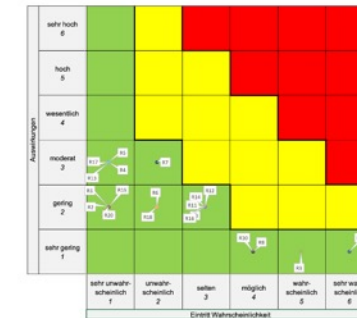


Abbildung 6: Screenshot Risikomatrix

### 8.2 Sicherheitsanforderungen und Risiko-Reduktion

Für die erkannten Risiken mit dem Status «gelb» wurden Massnahmen erarbeitet, welche die Risiken minimieren.

Nr.	Massnahme und Beschreibung	Reduktion des

## Art. 22 Datenschutz-Folgenabschätzung

<sup>1</sup> Der Verantwortliche erstellt vorgängig eine Datenschutz-Folgenabschätzung, wenn eine Bearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen kann. Sind mehrere ähnliche Bearbeitungsvorgänge geplant, so kann eine gemeinsame Abschätzung erstellt werden.

# Verzeichnis der Bearbeitungstätigkeiten

Gemäss § 23 Abs. 1 des Gesetzes über die Öffentlichkeit der Verwaltung und den Datenschutz vom 23. Mai 2007, SRSZ 140.410, ÖDSG) hat der Kanton über seine Datensammlungen ein öffentliches Register zu führen. Nicht in das Register werden Datensammlungen aufgenommen, die nur kurzfristig geführt werden, deren Inhalt rechtmässig veröffentlicht ist und die sich als reine Adresslisten darstellen (§ 23 Abs. 2 ÖDSG). Im Register nicht aufgeführt sind sodann die Personaldossiers, die in den Departementen, Ämtern und Anstalten geführt werden.

Quelle: Register der personenbezogenen Datensammlungen des Kantons Schwyz

## 1. Register der Datensammlungen

Das Informations- und Datenschutzgesetz (InfoDG, BGS 114.1) verlangt von jeder Behörde, dass sie ein Register ihrer eigenen Datensammlungen führt (§ 24 Abs. 1 InfoDG). Die Beauftragte für Information und Datenschutz führt das zentrale Register der Datensammlungen (§ 25 InfoDG). Das zentrale Register ergibt sich aus der Summe der Datensammlungen, welche die Behörden der Beauftragten für Information und Datenschutz melden.

Quelle: Erläuterungen zum Zentralen Register der Datensammlungen, Kanton Solothurn

- 13 -

Departementssekretariat

Datensammlung Nr. 1.0.3:

Bezeichnung	Einbürgerungen im kantonalen Verfahren
Rechtsgrundlage	Eidgenössische und kantonale Bürgerrechtsgesetzgebung (SR 141.0 / SRSZ 110.100)
Zweck	Geschäftskontrolle der ordentlichen und erleichterten Einbürgerungen, Wiedereinbürgerungen sowie Bürgerrechtsentlassungen; Dokumentation
Art der bearbeiteten Daten	Familien- und Vornamen, Staatsangehörigkeit, Heimort, Einbürgerungsgemeinde, Stand der Bearbeitung, Erledigung, Bemerkungen
Verantwortliche Stelle	Departement des Innern, Abt. Personenstand/ Bürgerrecht Tel. 041 819 16 10 / 11
Herkunft der Daten	von Betroffenen, von Dritten (Amtsstellen)
Bearbeitung durch Dritte	Zivilstandsämter, Gemeinderäte
Regelmässige Empfänger	Zivilstandsämter, Gemeinderäte
Zahl der betroffenen Personen	jährlich rund 1500

Quelle: Register der personenbezogenen Datensammlungen des Kantons Schwyz

# Checkliste für öffentliche Verwaltungen: Datenschutz und Datensicherheit im digitalen Bürgerdialog

Kostenloser Download

<https://konova.ch/publikation/checkliste-datenschutz>





E-Mitwirkung

# **E-Mitwirkung und Datenschutz**

# E-Mitwirkung und Datenschutz



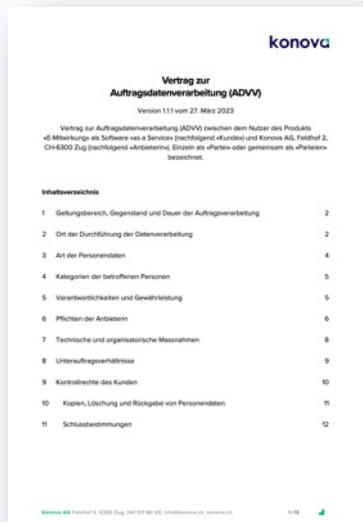
Technische und organisatorische Massnahmen



Unterstützung mit Know-How und Vorlagen



Sichere Cloud-Lösung, Betrieb in der Schweiz



## Empfehlung:

1

Bedarf für Anmeldung der Datenverarbeitung sowie ISDS-Konzept intern abklären.

2

Vertrag zur Auftragsdatenverarbeitung mit der Konova AG abschliessen.



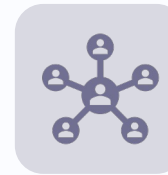
# Effiziente Online- Plattform für Dialog und Partizipation

In über 120 Gemeinden, Städten und Kantonen im Einsatz.

[www.e-mitwirkung.ch](http://www.e-mitwirkung.ch)



Projektkommunikation



Stakeholder-Management



Beteiligungsmodule



Intelligente Auswertung



**Fragen?**