

Nordwestschweizer Datenschutz-Aufsichtsbehörden, 24. August 2026 in Basel

Kritischer Aussenblick auf die Tätigkeit der Aufsichtsbehörden

Rechtsanwalt Martin Steiger





Private



www.digitale-gesellschaft.ch/event/datenschutz-fest



 **DIGITALE
GESELLSCHAFT**

Über uns ▾

Dossiers ▾

Unterstützen

Mitmachen

DE ▾



Freitag, 23. Oktober 2026 – Kulturhaus Helferei

DATENSCHUTZ-FESTIVAL 2026 – DATENSCHUTZ AUF DER HÖHE DER ZEIT

DATENSCHUTZ FESTIVAL

Wie bleiben der Schutz der Daten und die Selbstbestimmung über unser vernetztes Leben auf der Höhe der Zeit? Diese Frage diskutieren wir am fünften Datenschutz-Festival mit dem EDÖB als Spezialgast. Das diesjährige Datenschutz-Festival der Digitalen Gesellschaft findet am Freitag, 23. Oktober 2026 ab 14.15 Uhr in **Zürich** im **Kulturhaus Helferei** statt.

Technologien entwickeln sich rasant und sie durchdringen unser Lebens immer stärker. Fortlaufend entstehen mehr und neue Daten, die von Behörden und Unternehmen über uns gesammelt und bearbeitet werden. Darüber diskutieren wir am Datenschutz-Festival – auch erneut im direkten Austausch mit Dr. Adrian Lobsiger, dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB).

Seit dem ersten Datenschutz-Festivals im Jahr 2022 setzen wir uns mit den Grundlagen und Schutzzielen eines verantwortungsvollen Datenschutzes auseinander. Denn wir sind überzeugt: Datenschutz und Datennutzung gehören zusammen.



**UNTER-
STÜTZEN**

Dein Schlüssel. Deine Daten.

Spende jetzt für ein sicheres und selbstbestimmtes Gesundheitsdossier!

8%

Bereits 1'964 von 23'000 Franken

noch 43 Tage

Unterstützen

NEWSLETTER

Name (optional)

E-Mail

Abonnieren

abmelden

SERVICE

Heute: Kritischer Aussenblick auf die
Tätigkeit der Nordwestschweizer
Datenschutz-Aufsichtsbehörden

- **Zuerst:** Fokus auf Kommunikation, künstliche Intelligenz und digitale Souveränität
- **Danach:** Diskussion, Fragen und Widerspruch

Kommunikation

Öffentlichkeit: Ist überhaupt bekannt, dass es Datenschutz-Aufsichtsbehörden gibt?

Mehr Bekanntheit ➡ Mehr Wirkung



Private



eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52024



EUROPÄISCHE KOMMISSION

Brüssel, den 25.7.2024

COM(2024) 357 final

MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT

Zweiter Bericht zur Anwendung der Datenschutz-Grundverordnung (DSGVO)

1 EINLEITUNG

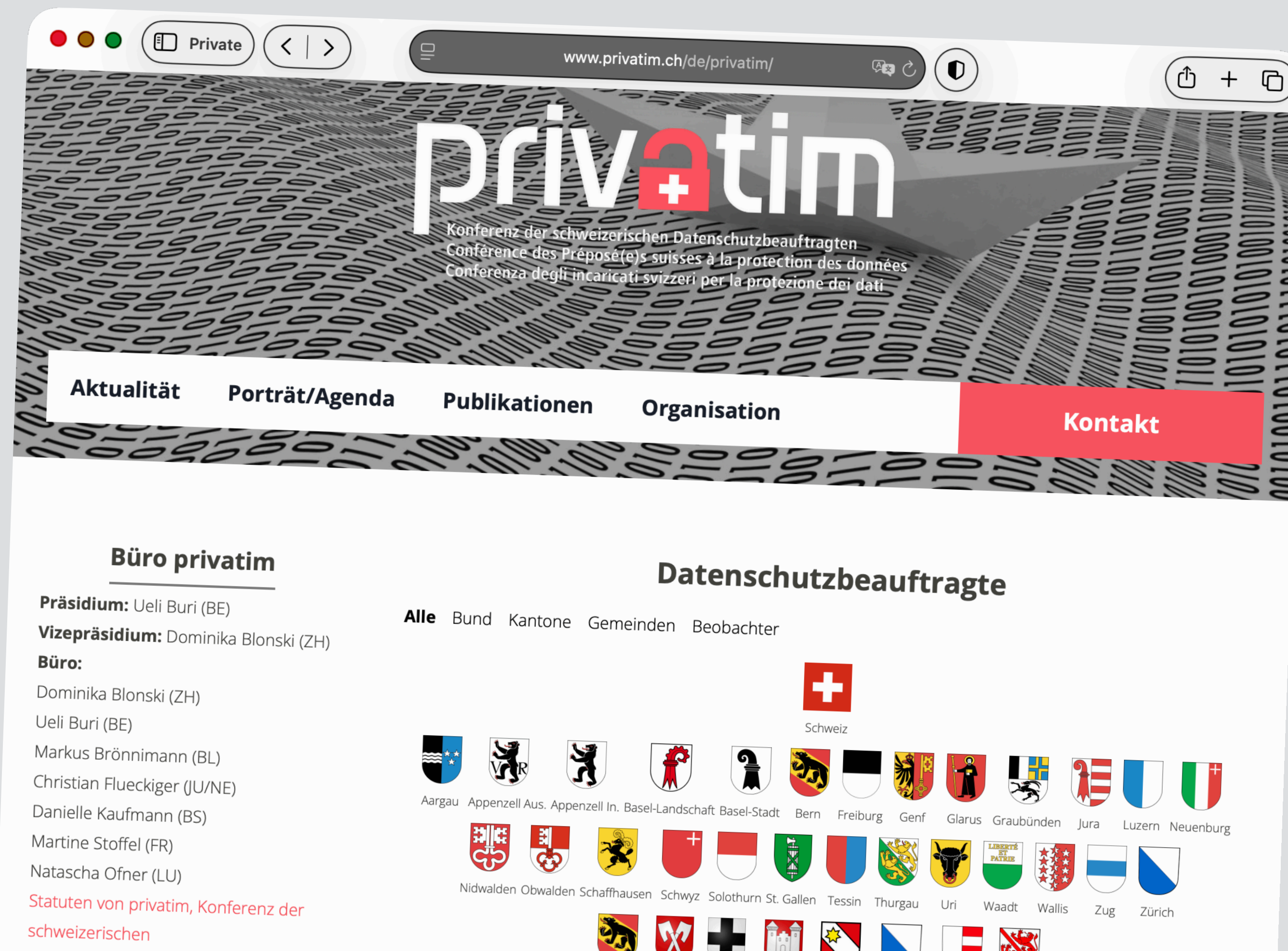
Der vorliegende Bericht ist der zweite Bericht der Kommission über die Anwendung der Datenschutz-Grundverordnung (DSGVO), der gemäß Artikel 97 DSGVO angenommen wurde. Der erste Bericht wurde am 24. Juni 2020 angenommen (im Folgenden „Bericht 2020“¹).

Die DSGVO ist einer der Eckpfeiler des Ansatzes der EU für den digitalen Wandel. Ihre Grundsätze – eine faire, sichere und transparente Verarbeitung personenbezogener Daten, die sicherstellt, dass Einzelpersonen die Kontrolle behalten – liegen allen EU-Maßnahmen zugrunde, die die Verarbeitung personenbezogener Daten betreffen.

Seit dem Bericht 2020 hat die EU eine Reihe von Initiativen angenommen, mit denen die Einzelnen in den Mittelpunkt des digitalen Wandels gestellt werden sollen. Jede Initiative verfolgt ein besonderes Ziel, wie die Schaffung eines sichereren Online-Umfelds, eine gerechtere und wettbewerbsfähigere digitale Wirtschaft, die Erleichterung bahnbrechender Forschung, die Sicherstellung der Entwicklung einer sicheren und vertrauenswürdigen künstlichen Intelligenz (KI) und die Schaffung eines sicheren digitalen Umfelds für Daten. Solche Initiativen sind Teil der EU-Initiative für die DSGVO. Die

- *«72 % der Befragten in der gesamten EU gaben an, von der DSGVO gehört zu haben, darunter 40 %, die wissen, worum es sich dabei handelt.»*
- *«68 % der Befragten in der EU geben an, von einer nationalen Behörde gehört zu haben, die für den Schutz ihrer Datenschutzrechte zuständig ist, wobei 24 % aller Befragten angeben, dass sie auch wissen, welche Behörde zuständig ist.»*

Betroffene Personen: «Wer ist für mich überhaupt zuständig?»



Zuständigkeitsfinder privatim

+

< > ↺

File

MOCKUP · KONZEPTDEMONSTRATION

Kein Angebot von privatim. Behördenbezeichnungen, Fundstellen und Kontaktangaben sind Demo-Material für einen Vortrag.

Konferenz der schweizerischen Datenschutzbeauftragten

Deutsch

Français

Italiano

privatim

Konferenz der schweizerischen Datenschutzbeauftragten

Zuständigkeitsfinder für betroffene Personen · ein gemeinsames Angebot der kantonalen und kommunalen Aufsichtsbehörden

privatim

Zuständigkeit finden

Mitgliedsbehörden

Stellungnahmen

Merkblätter

Veranstaltungen

AUSKUNFT FÜR BETROFFENE PERSONEN

Bund, Kanton oder Ausland – wer beaufsichtigt Ihren Fall?

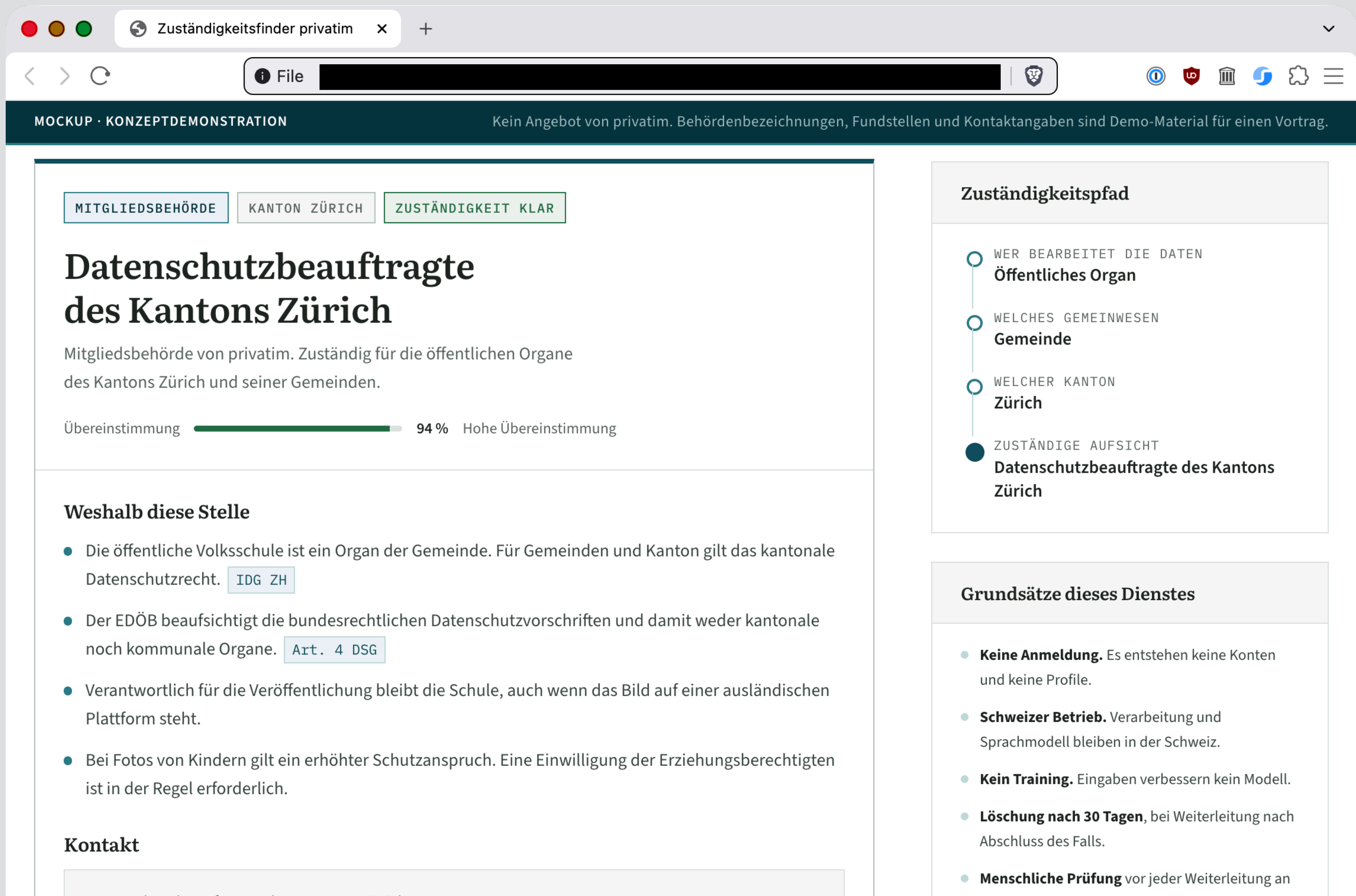
Wer in der Schweiz Datenschutz durchsetzen will, muss zuerst die richtige Stelle finden. Für kantonale und kommunale Organe sind unsere Mitgliedsbehörden zuständig, für Bundesorgane und private Unternehmen der EDÖB. Schildern Sie Ihren Fall in eigenen Worten – wir sagen Ihnen, wohin er gehört, und leiten ihn auf

Wer hinter diesem Angebot steht

privatim ist der Zusammenschluss der kantonalen und kommunalen Datenschutzbeauftragten der Schweiz. Die Mitgliedsbehörden beaufsichtigen die öffentlichen Organe ihres Kantons und beraten betroffene Personen kostenlos.

Dieser Dienst ordnet Ihren Fall der zuständigen Stelle zu. Er ersetzt weder eine Rechtsberatung noch einen Entscheid der Behörde.

Betrieb auf Schweizer Infrastruktur · Auswertung mit einem in der Schweiz betriebenen Sprachmodell · keine Weitergabe an Dritte



MITGLIEDSBEHÖRDE

KANTON ZÜRICH

ZUSTÄNDIGKEIT KLAR

Datenschutzbeauftragte des Kantons Zürich

Mitgliedsbehörde von privatim. Zuständig für die öffentlichen Organe des Kantons Zürich und seiner Gemeinden.

Übereinstimmung 94 % Hohe Übereinstimmung

Weshalb diese Stelle

- Die öffentliche Volksschule ist ein Organ der Gemeinde. Für Gemeinden und Kanton gilt das kantonale Datenschutzrecht. IDG ZH
- Der EDÖB beaufsichtigt die bundesrechtlichen Datenschutzvorschriften und damit weder kantonale noch kommunale Organe. Art. 4 DSG
- Verantwortlich für die Veröffentlichung bleibt die Schule, auch wenn das Bild auf einer ausländischen Plattform steht.
- Bei Fotos von Kindern gilt ein erhöhter Schutzanspruch. Eine Einwilligung der Erziehungsberechtigten ist in der Regel erforderlich.

Kontakt

Zuständigkeitspfad

- WER BEARBEITET DIE DATEN
Öffentliches Organ
- WELCHES GEMEINWESEN
Gemeinde
- WELCHER KANTON
Zürich
- ZUSTÄNDIGE AUFSICHT
Datenschutzbeauftragte des Kantons Zürich

Grundsätze dieses Dienstes

- Keine Anmeldung.** Es entstehen keine Konten und keine Profile.
- Schweizer Betrieb.** Verarbeitung und Sprachmodell bleiben in der Schweiz.
- Kein Training.** Eingaben verbessern kein Modell.
- Löschung nach 30 Tagen,** bei Weiterleitung nach Abschluss des Falls.
- Menschliche Prüfung** vor jeder Weiterleitung an

Heutige öffentliche Kommunikation:

- **In erster Linie mit «Pull»:** Websites, die man besuchen muss, Publikationen, die man finden muss, Behörden, die man kontaktieren muss, ...
- **«Push» wenig ausgeprägt:** Massenmedien, Newsletter, Publikationen, Social-Media, Veranstaltungen, ...

Praktische Hilfe: Muster / Vorlagen
teilweise vorhanden, aber wo bleiben
die digitalen Hilfsmittel?

AutoSave

Auskunftsbegeh... — Saved to my Mac

Comments

Editing

Share

HomeInsertDrawDesignLayoutReviewViewDeveloper

PasteClipboard

FontFrutiger LT...8A^A~AaA

ParagraphListBulletedListNumberedListDecreaseIndentIncreaseIndentTextAlignJustifyCenterAlignLeftAlignRightLinkUnlinkTableBorder

StylesStyles PaneDictateAdd-insEditor

Absender:
Vorname/Name →
Adresse →
PLZ/Ort →

→
→ Adresse der
Behörde →
.....
.....
.....
→ Ort und Datum →

Auskunftsbegehren gemäss § 26 des Informations- und Datenschutzgesetzes (InfoDG)

Sehr geehrte Damen und Herren

Bitte geben Sie mir schriftlich Auskunft, welche Daten über mich bearbeitet werden im Zusammenhang mit:

.....(genauer Zusammenhang einfügen)

Ich bitte Sie, mir die Vollständigkeit und Richtigkeit der zugestellten Unterlagen zu bestätigen.

Vielen Dank für Ihre Bemühungen.

■ Freundliche Grüsse

..... → Unterschrift

Page 1 of 176 wordsGerman (Switzerland)

Focus

160%



**Finde heraus,
was Unternehmen,
Organisationen
und Behörden
über Dich wissen.**

Du hast das Recht zu erfahren, ob ein Unternehmen, eine Organisation oder eine Behörde Personendaten über Dich bearbeitet, welche Daten bearbeitet werden, wofür die Daten verwendet werden und woher die Daten stammen. Wir helfen Dir mit diesem Generator, dieses Recht zu nutzen und ein Auskunftsbegleichen an den jeweiligen Verantwortlichen zu richten.

Gib mir

Kantonspolizei Basel-Stadt

Clarastrasse 38, 4058 Basel

Justiz- und Sicherheitsdepartement Basel-Stadt, Kantonspolizei

Spiegelgasse 6, 4051 Basel

Worum es geht

Das schweizerische Datenschutzrecht gibt Dir ein Recht auf Auskunft. Unternehmen, Organisationen und Behörden, die Personendaten über Dich bearbeiten, müssen Dir auf Anfrage darüber Auskunft erteilen, welche Daten sie bearbeiten, wofür sie verwendet werden, woher sie stammen, wie lange sie aufbewahrt werden und an wen sie weitergegeben werden. Die Auskunft hilft Dir zu verstehen, welche Datensammlungen über Dich bestehen und ob Du weitere Rechte wie Widerspruch, Löschung oder Berichtigung nutzen möchtest.

So läuft die Anfrage ab

1. **Unternehmen, Organisation oder Behörde finden:** Suche einen schweizerischen

Websites: «Gefangen» im
kantonalen Online-Auftritt



Private



www.bs.ch/datenschutzbeauftragte



Kanton Basel-Stadt

Themen

Organisation

DE ▾

ePortal ↗



Datenschutzbeauftragte

Die Datenschutzbeauftragte des Kantons Basel-Stadt ist eine unabhängige Aufsichtsbehörde. Sie nimmt Aufgaben im Bereich des Datenschutzrechts und des Öffentlichkeitsprinzips wahr, mit dem Ziel die Grundrechte der Menschen im Kanton Basel-Stadt zu schützen. Insbesondere berät sie öffentliche Organe zum rechtmässigen Umgang mit Informationen sowie Private zu ihren Rechten,

Zu statistischen Zwecken und zur Verbesserung unseres Angebots werden Informationen, die uns ihr Zugangsggerät und ihr Browser beim Aufruf dieser Webseite automatisch mitteilt, erfasst und bearbeitet. Dieser Vorgang erfolgt anonymisiert und entfernt somit den Bezug zu Ihrer Person.

Ihre Daten werden ausschliesslich von uns verwendet. Eine Weitergabe an Dritte erfolgt nicht.

Weitere Informationen finden Sie in unserer **Datenschutzerklärung**.

✓ Weiter mit allen Cookies

✓ Weiter mit erforderlichen Cookies



Private



www.bs.ch/datenschutzerklaerung



Kanton Basel-Stadt

Themen

Organisation

DE ▾

ePortal ↗



Datenschutzerklärung

Auf dieser Seite

↓ **Rechtliche Hinweise
zur Benützung des
Internet-Angebots des**

↓ **Benutzung der Websites**

↓ **Haftungsausschluss**

Zu statistischen Zwecken und zur Verbesserung unseres Angebots werden Informationen, die uns ihr Zugangsgerät und ihr Browser beim Aufruf dieser Webseite automatisch mitteilt, erfasst und bearbeitet. Dieser Vorgang erfolgt anonymisiert und entfernt somit den Bezug zu Ihrer Person.

Ihre Daten werden ausschliesslich von uns verwendet. Eine Weitergabe an Dritte erfolgt nicht.

Weitere Informationen finden Sie in unserer **Datenschutzerklärung**.

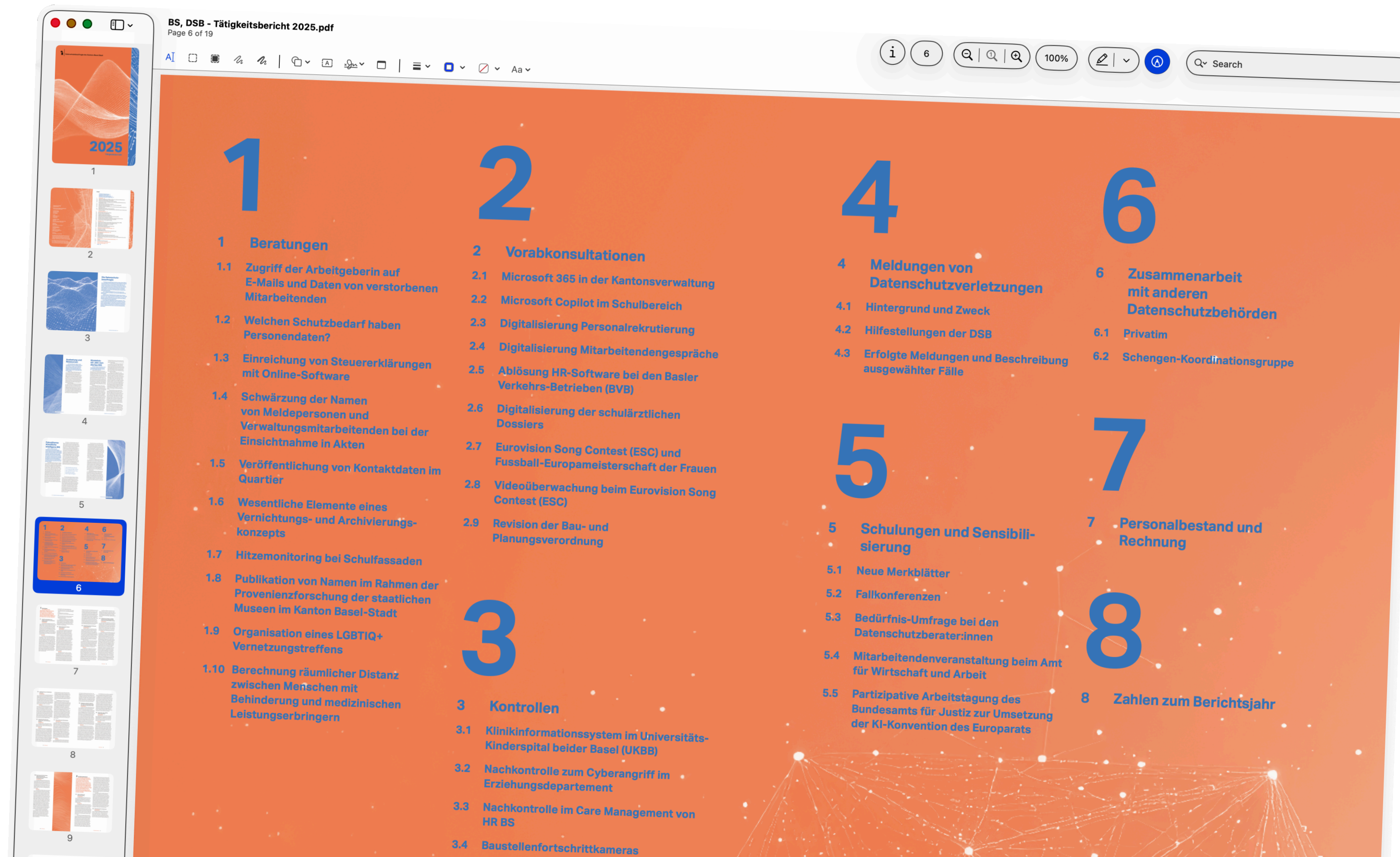
✓ Weiter mit allen Cookies

✓ Weiter mit erforderlichen Cookies

Informelle Umfrage zu Websites:

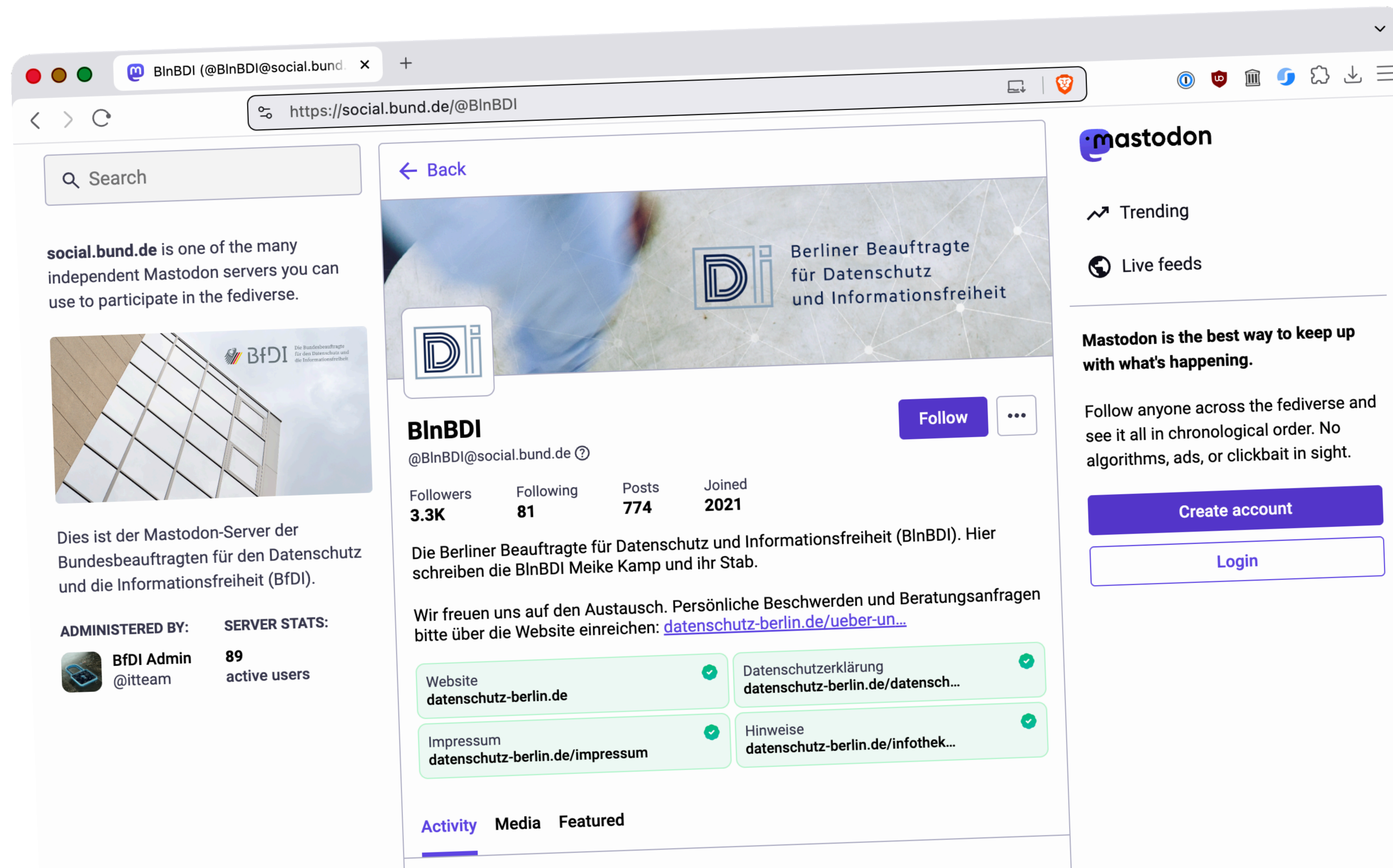
- *«Ich finde die Website sehr unübersichtlich. Mir ist nicht klar, was ich wo finden kann.»*
- *«Nicht viel Hilfreiches, vor allem kaum Muster. Juristen-Deutsch.»*
- *«Nutzt bei denen niemand ein Smartphone?»*
- *«Wer ist die Zielgruppe? Wer sind die Zielgruppen?»*
- *«Visuell nicht sehr ansprechend. Viel zu viel Text».*
- *«Ich fand den Tätigkeitsbericht nur mit ChatGPT.»*

Es gibt so viel zu erzählen!



Ärgernis: Kein «Open Access» bei
Publikationen und Veranstaltungen

«Open Access»: Mögliche Vorbildfunktion auch bei Social-Media



Idealfall: Transparenz und mehr «Push»
in der öffentlichen Kommunikation!

Mehrfache Verwertung der vielen
ohnehin vorhandenen Inhalte

Künstliche Intelligenz

KI: Ist die heutige Realität schon bei den
Datenschutz-Aufsichtsbehörden
angekommen?

Gleichzeitig beobachtet die DSB, dass unter den Mitarbeitenden der öffentlichen Organe weiterhin viele offene Fragen im Zusammenhang mit KI bestehen. Auch der Umgang mit dem Thema variiert stark von Organ zu Organ. Soweit es ihre Ressourcen zulassen, wird die DSB weiterhin darauf hinwirken, die Sensibilisierung für den Datenschutz beim Einsatz von KI-Anwendungen zu fördern. Ferner wird sie sich für eine angemessene Regulierung einsetzen, welche die Grundrechte der betroffenen Personen vor KI-Risiken schützt.

KI ≠ Chatbot:

- Chatbot ➡ Copilot ➡ Agent ➡ «AI Workforce» 🔥
- Umfassender Zugriff auf Akten, E-Mails, externe / interne Datenbanken, ...
- Neue Sicherheitsrisiken wie Datenabfluss, «Prompt Injection», «Schatten-KI», «Vibe Coding», ...
- Autonomie vs. Verantwortung: Was bleibt von der Forderung «Human in the Loop» noch übrig? 🔥

claude.com/blog/auto-mode-default-in-claude-code

Claude

Contact salesTry Claude

Blog / Auto mode is now the default in Claude Code for Pro, Max, and Team plans

Explore here

Auto mode is now the default in Claude Code for Pro, Max, and Team plans

Claude Code will soon run auto mode by default for Pro, Max, and Team plans, enabling longer-running autonomous work, and catching more dangerous commands than manual review in our testing.

Category

Claude Code

Product

Claude Code

Date

August 7, 2026

Reading time

11 min

Share

Copy link

We're making auto mode the default in Claude Code. Starting on August 14, new sessions on Pro, Max, and Team plans will run in auto mode. If you've already set a different default yourself, you may get a one-time prompt asking whether you want to switch to auto mode. If you have a pinned default, nothing changes for you. The auto mode classifier uses a small number of extra tokens per tool call, and we're no longer charging Claude Code users on Pro.

claude.com/blog/auto-mode-default-in-claude-code

Claude

Contact salesTry Claude

Blog / Auto mode is now the default in Claude Code for Pro, Max, and Team plans

Explore here

Data suggests that manual review can become habitual: users approve 97% of permission prompts in Claude Code. While most prompts are likely for safe, routine commands, an approval rate that high suggests many users are clicking through reflexively rather than reviewing each command. These prompts ask developers to make dozens or hundreds of important security decisions every day, often in the middle of projects, which places the review burden on users and increases the chance that something important slips through the cracks. Data also suggests that users more frequently scrutinize and push back on other types of dialogues: for example, when Claude presents a plan for approval, users reject 39% of them. But for individual permissions requests, the rejection rate is only 3%.

The same pattern shows up in settings files. As of June 2026, 49.5% of active CLI users have manually created a Bash allow-rule—5% allow any shell command outright, and another 43% have interpreter rules like `Bash(python:*)` or `Bash(node:*)` that are essentially equivalent in practice—and that share is growing roughly 5 percentage points every 5 weeks. Beyond allow-rules, 62% of users have used `bypassPermissions` or clicked “don’t ask again” on Bash, and 25% of interactive sessions start in bypass permissions mode.

Permission rules still fire before the classifier in auto mode, except for allow rules broad enough to grant arbitrary code execution (e.g. `python:*`). These arbitrary rules are set aside while in auto mode, since they would let commands skip the classifier entirely. Settings files aren’t modified, and the rules apply again the moment you switch to another mode.

Improving safety with auto mode

Research conducted internally and through several third parties suggests that auto mode is safer than how a typical user engages

«[...] in einer Aargauer Sekundarschule erstellt
eine künstliche Intelligenz von jedem Kind ein
Profil [...].»



Idealfall: Datenschutzrechtliche Risiken
benennen, aber vor allem einen
rechtmässigen KI-Einsatz aufzeigen
und sicherstellen, auch
beim «Outsourcing»

Digitale Souveränität

Digitale Souveränität: *«Erforderliche Kontroll- und Handlungsfähigkeit im digitalen Raum, um die Erfüllung staatlicher Aufgaben sicherzustellen»*

Bundesrat: Bericht zur Digitalen Souveränität der Schweiz,
Medienmitteilung, 26. November 2025

Deshalb: Souveränität $\neq$ Autarkie

Medienmitteilung der Datenschutzbeauftragten des Kantons Basel-Stadt zu M365

08.04.2025 - 15:30

News

Die Datenschutzbeauftragte des Kantons Basel-Stadt bedauert den Entscheid des Regierungsrates zur umfassenden Einführung der Microsoft 365 Cloud (M365) in der kantonalen Verwaltung. Sie sieht darin eine erhebliche Schwächung der digitalen Souveränität und eine Gefährdung für die Grundrechte der Menschen im Kanton Basel-Stadt.

Im Vorfeld zum Entscheid hatte die Datenschutzbeauftragte wiederholt von einer umfassenden Einführung der Microsoft 365 Cloud (M365) abgeraten. Sie hat den Regierungsrat in mehreren Stellungnahmen auf die damit verbundenen gewichtigen Risiken aufmerksam gemacht. Mit der Auslagerung der gesamten ICT-Grundversorgung, inklusive E-Mail-Kommunikation, Telefonie und Datenablage, verliert der Kanton einen



Resolution zur Auslagerung von Datenbearbeitungen in die Cloud

Cloudbasierte Software erscheint heute als so attraktiv wie nie. Infrastrukturen, die potenziell allen Internet-Usern zur Verfügung stehen (sog. «Public Clouds»), erlauben eine dynamische Zuweisung von Rechen- und Speicherleistungen nach dem jeweiligen Bedarf der Kunden. Dieser Skaleneffekt ist umso grösser, je weitreichender – und in der Regel auch internationaler – die Infrastruktur des Cloud-Anbieters ist (man denke an sogenannte «Hyperscaler» wie Microsoft, Google oder Amazon). Nebst Einzelpersonen und Privatunternehmen greifen auch immer mehr öffentliche Organe auf zur direkten Nutzung bereitgestellte Anwendungen («Software-as-a-Service», kurz: SaaS) solcher Anbieter zurück. Auch lässt sich beobachten, dass Anbieter ihre Kunden vermehrt in die Cloud zu drängen versuchen.

Allerdings tragen öffentliche Organe eine besondere Verantwortung gegenüber den Daten ihrer Bürgerinnen und Bürger. Zwar dürfen sie deren Bearbeitung an Dritte auslagern, müssen dabei aber sicherstellen, dass der Datenschutz und die Informationssicherheit gewahrt bleiben. Vor einer Auslagerung von Personendaten in Cloud-Dienste müssen die Behörden deshalb unabhängig von der Sensitivität der Daten die besonderen Risiken im Einzelfall analysieren und mit geeigneten Massnahmen auf ein tragbares Mass reduzieren (vgl. Cloud-Merkblatt von privatim).

«Aus folgenden Gründen hält privatim die Auslagerung von besonders schützenswerten oder einer gesetzlichen Geheimhaltungspflicht unterstehenden Personendaten in SaaS-Lösungen von grossen internationalen Anbietern durch öffentliche Organe in den meisten Fällen (wie namentlich M365) für unzulässig [...].»

privatim: Resolution «Auslagerung von Datenbearbeitungen in die Cloud», 24. November 2025

«**Fazit:** Die Nutzung internationaler SaaS-Lösungen für besonders schützenswerte oder einer gesetzlichen Geheimhaltungspflicht unterstehende Personendaten durch öffentliche Organe ist nur dann möglich, wenn die Daten vom verantwortlichen Organ selbst verschlüsselt werden und der Cloud-Anbieter keinen Zugang zum Schlüssel hat.»

privatim: Resolution «Auslagerung von Datenbearbeitungen in die Cloud», 24. November 2025

Gleichzeitig: Microsoft 365 wird bereits
im grossen Stil eingesetzt und weiter
ausgerollt, bevorzugt mit «Labeling»

Ergebnis: Verunsicherung bei Behörden
und betroffenen Personen

§ 46 Empfehlungen

¹ Die oder der Datenschutzbeauftragte kann zum Umgang mit Informationen Empfehlungen abgeben.

² Das öffentliche Organ, an welches die Empfehlung gerichtet ist, hat gegenüber der oder dem Datenschutzbeauftragten zu erklären, ob es der Empfehlung folgen will.

§ 47 Weisungen zum Bearbeiten von Personendaten

¹ Wenn ein öffentliches Organ erklärt, der Empfehlung der oder des Datenschutzbeauftragten nicht folgen zu wollen, oder tatsächlich der Empfehlung nicht folgt, kann die oder der Datenschutzbeauftragte die Empfehlung oder Teile davon als Weisung in Form einer Verfügung erlassen, wenn

- a) die Empfehlung das Bearbeiten von Personendaten betrifft und
- b) das Interesse an der Durchsetzung schwer wiegt.

² Keine Weisung kann gegenüber dem Appellationsgericht erlassen werden.

³ Die oder der Datenschutzbeauftragte kann direkt eine Weisung erlassen, wenn absehbar ist, dass das öffentliche Organ eine Empfehlung ablehnen oder ihr keine Folge leisten wird.

⁴ Werden schutzwürdige Interessen offensichtlich gefährdet oder verletzt, so kann die oder der Datenschutzbeauftragte anordnen, dass das öffentliche Organ die Bearbeitung bis zur erfolgten Überprüfung durch das Appellationsgericht einschränkt oder einstellt.

⁵ Das öffentliche Organ, an welches die Weisung gerichtet ist, kann sie mit einem Rekurs nach den allgemeinen Vorschriften

Vertrauensfrage: Starke öffentliche
Warnung, aber was folgt konkret?

Wo endet die Aufsicht und
wo beginnt die Politik?

Auch: Was ist die tatsächliche Rechtslage?

Ist in der Schweiz wirklich alles besser?

Was taugen die Alternativen wirklich?

Wieso beurteilen wir ausländische

Zugriffsrisiken je nach Staat

so unterschiedlich?

Idealfall: Wer als Datenschutz-Aufsichtsbehörde «unzulässig» sagt, muss auch erklären, was aufsichtsrechtlich daraus folgt

Wunschzettel 

- **Kommunikation:** Mehr «Push», konsequent «Open Access» und eigenständige Online-Präsenz
- **Künstliche Intelligenz:** Rechtmässigen Einsatz aufzeigen und sicherstellen, auch beim «Outsourcing»
- **Digitale Souveränität:** Geltendes Recht durchsetzen und dabei Datenschutzaufsicht und Digitalpolitik klar auseinanderhalten

Diskussion, Fragen und Widerspruch

martinsteiger.ch 🙏