

# Vernehmlassungsantwort der Piratenpartei beider Basel zur Änderung des IDG

Datenschutz und Transparenz sind seit der Gründung der Piratenpartei beider Basel, der Piratenpartei Schweiz, der Europäischen Piratenpartei und der Pirate Parties International ein Kernthema der Piratenpolitik<sup>1</sup>. Insofern beobachten wir die Änderungen im IDG mit grossem Interesse und fühlen uns zu einer Stellungnahme verpflichtet.

## Allgemeines

Die Anpassungen an die EU-Verordnung 2016/679 (DSGVO) und die EU-Richtlinie 2016/680 begrüssen wir ausdrücklich. Im Kanton Baselland, wie auch im Rest der Schweiz, ist die Revision überfällig. Die Digitalisierung schreitet schnell voran und es ist unglaublich wichtig, dass die Behörden und der Datenschutz Schritt halten können.

## Fehlender Open Data Grundsatz

Leider stellen wir fest, dass im Bereich der Informationstätigkeit keine wesentlichen Anpassungen vorgenommen wurden. Die Piratenpartei beider Basel fordert eine grundsätzliche Open Data-Strategie<sup>2</sup> für öffentliche Datenbestände und Informationen von öffentlichem Interesse. Konkret fordern wir:

- Proaktive öffentliche Bekanntgabe von Daten, Dokumenten, Statistiken usw.
- Freie Lizenzen<sup>3</sup>, die die Weiterbearbeitung ermöglichen
- Freie Datenformate<sup>4</sup>, Schnittstellen und Standards
- Barrierefreie Zugänge<sup>5</sup>
- Automatisierte Abrufmöglichkeit und maschinenlesbare Formate
- Anonymer und kostenloser Zugang
- Sicherstellung der Aktualität und Integrität
- Förderung von gemeinnützigen Projekten, die öffentliche Datenbestände bearbeiten
- Zusammenarbeit über die Kantons Grenzen hinweg

Während sich Bundesorgane, andere Kantone (bspw. BS oder ZH)<sup>6</sup> und die EU<sup>7</sup> immer stärker in diesem Bereich engagieren, gerät der Kanton Baselland hier zunehmend ins Hintertreffen. Die Chance, einen Open Data-Grundsatz gesetzlich festzuschreiben, wurde in dieser Revision verpasst.

---

1 <https://www.piratenpartei.ch/parteiprogramm/>

2 <https://okfn.org/opendata/>

3 <https://www.gnu.org/licenses/licenses.de.html>

4 <https://jimmywales.com/2004/10/21/free-knowledge-requires-free-software-and-free-file-formats/>

5 <https://www.edi.admin.ch/edi/de/home/fachstellen/ebgb/e-accessibility-/communicationnumeriqueaccessible2.html>

6 <https://opendata.swiss/de/organization>

7 <https://data.europa.eu/euodp/de/about>

## **Videüberwachung im öffentlichen Raum**

Wir bedauern, dass die Videüberwachung im öffentlichen Raum nicht restriktiver geregelt wurde. Im Vergleich zum IDG Basel-Stadt (§ 18) regelt der Kanton Baselland diesen, nach unserer Meinung sehr sensiblen Bereich, nur im Polizeigesetz und mit wesentlich lascheren Bestimmungen. Wir bezweifeln, dass so eine unabhängige Beurteilung und ein angemessener Schutz möglich ist.

Wir fordern, dass die Wirksamkeit und Verhältnismässigkeit von Videüberwachung im öffentlichen Raum regelmässig nachgewiesen werden muss und die Bearbeitung der dabei anfallenden Personendaten strikter geregelt wird.

Wir glauben auch, dass andere Sensoren (z.B. Brandmelder), bei denen gar keine Personendaten anfallen, sich für bestimmte Anforderungen besser eignen würden.

## **Datenschutzbeauftragte\*r**

Während der Umfang der Informationen und Personendaten und die damit verbundenen Risiken in den letzten Jahren, angetrieben von der Digitalisierung, stark angestiegen ist, haben sich die Mittel und Kompetenzen der/des Datenschutzbeauftragten kaum verändert. Die Piratenpartei beider Basel befürchtet, dass die/des Datenschutzbeauftragte\*r so nicht mehr alle Aufgaben mit der notwendigen Sorgfalt oder in nützlicher Frist erledigen kann.

Für die Durchsetzung des Informations- und Datenschutzgesetzes halten wir es für unabdingbar, dass die finanziellen und personellen Mittel der Aufsichtsbehörde aufgestockt werden. Dies fordert im Übrigen auch die Konferenz der schweizerischen Datenschutzbeauftragten.<sup>8</sup>

## **Strafbestimmungen**

Mit dem gesteigerten Umfang und Risiko der Datenbestände sind auch die Konsequenzen bei widerrechtlichem oder verantwortungslosen Umgang mit (besonderen) Personendaten gestiegen. Das Abhandenkommen ganzer Datenbanken oder Zugänge zu den Datenbeständen durch Dritte<sup>9</sup>, sowie der damit verbundene Vertrauensverlust, ist mit einem Bussgeld kaum wiedergutzumachen. Zumal Bussgelder üblicherweise wieder einem öffentlichen Organ selbst zugute kommen.<sup>10</sup>

## **Stellungnahmen zu einzelnen Änderungen**

### **§ 3 Begriffe Absatz 2**

Wir begrüssen die Streichung des Begriffs «Rassenzugehörigkeit» ausdrücklich

---

8 <https://www.privatim.ch/de/resolution-fehlende-ressourcen-bei-den-datenschutzbehorden/>

9 <https://www.robin-data.io/datenschutz-akademie/news/beispiele-fuer-datenpannen-im-datenschutz>

10 <https://www.lto.de/recht/justiz/j/vg-stuttgart-17k525519-luftreinhalteplan-fahrverbot-deutsche-umwelthilfe-zwangsgeld-gemeinnuetzige-private-organisation-kinderkrebsstiftung/>

### **§ 3 Begriffe Absatz 5**

Wir begrüssen die Aufnahme biometrischer Daten in die Definition.

Leider werden diese Daten vermehrt zur Authentifizierung zugangsberechtigter Personen verwendet (z. B. Fingerabdruckscanner), ungeachtet dessen, dass die Daten gegen den Willen der Person verwendet werden können und eine Änderung beim Bekanntwerden nicht möglich ist.

### **§ 3 Begriffe Absatz 7**

*Profiling ist jede Auswertung von Informationen oder Personendaten, um wesentliche persönliche Merkmale zu analysieren oder Entwicklungen vorherzusagen, insbesondere bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, Intimsphäre oder Mobilität.*

Die Definition ist uns etwas zu eng gefasst. Profiling kann auch bedeuten, konkrete Handlungen vorherzusagen (Artikel 4 Absatz 4 DSGVO), gezielt Einfluss zu nehmen, präventive Massnahmen zu treffen oder automatisierte Entscheidungen zu fällen. Das Profiling darf keinesfalls mit Grundrechten wie der Unschuldsvermutung, Rechtsgleichheit oder der persönlichen Freiheit kollidieren.

### **Automatisiertes Bearbeiten von Personendaten**

Der Entwurf zur Totalrevision des Bundesgesetz über den Datenschutz (E-DSG) definiert Profiling zudem als automatisiert bearbeitete Personendaten (Artikel 4 Literal f). Zusätzlich besagt Artikel 19 E-DSG, dass automatisierte Entscheidungen gekennzeichnet werden müssen und die betroffene Person die Überprüfung des Entscheids durch eine natürliche Person verlangen kann. Beides ist aus unseres Sicht unabdingbar, wenn der Kanton Baselland Personendaten automatisiert Bearbeiten möchte.

Ausserdem fordern wir, dass die Algorithmen und Quellcodes von Software veröffentlicht werden müssen, sodass das automatisierte Bearbeiten und daraus abgeleitete Entscheide und Handlungen nachvollzogen werden können.<sup>11</sup>

### **§ 9a Absatz 3**

*Pilotprojekte sind auf maximal fünf Jahre zu befristen.*

Insbesondere im digitalen Bereich sind fünf Jahre eine sehr lange Zeit und die Entwicklungen im Vorhinein nicht absehbar. Viele Softwareprojekte und digitale Schutzmassnahmen überdauern eine solche Frist gar nicht oder ändern sich in dieser Zeit grundlegend.

Zum Vergleich: Im Entwurf zur Totalrevision des Bundesgesetz über den Datenschutz ist ein Evaluationsbericht nach spätestens zwei Jahren vorgesehen (Artikel 31 Absatz 3 E-DSG). Der Paragraf wurde mehrheitlich aus dem § 9a IDG Basel-Stadt übernommen, wo die Revision des Gesetzes jedoch noch bevorsteht.

Wir schlagen vor, Pilotprojekte auf drei Jahre zu befristen und jährlich mit der/dem kantonalen Datenschutzbeauftragten zu evaluieren.

<sup>11</sup> Orwat, Carsten (2019): Diskriminierungsrisiken durch Verwendung von Algorithmen, S. 97

## § 11a Absatz 3

*Die Folgenabschätzung enthält mindestens:*

- a. *eine Beschreibung der geplanten Bearbeitungsvorgänge,*
- b. *eine Bewertung der in Bezug auf die Grundrechte der betroffenen Personen bestehenden Risiken sowie*
- c. *eine Darstellung und Bewertung der geplanten organisatorischen und technischen Abhilfemassnahmen, Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz der Grundrechte der betroffenen Personen sichergestellt und der Nachweis erbracht werden soll, dass die Datenschutzbestimmungen eingehalten werden.*

In Anbetracht des breiten Einsatzes digitaler Systeme, Cloud Computing<sup>12</sup> und dem digitalen Wettrüsten wünschen wir uns ein gesetzlich vorgeschriebenes Rahmenkonzept für den Ausfall, die Kompromittierung und Unabhängigkeit der Systeme.

Bisher ist dies nur rudimentär in der Verordnung § 19 VIS geregelt. Da die Formulierung in der Verordnung sehr allgemein gehalten ist, wäre eine Übertragung ins Gesetz vorstellbar. Die Verordnung müsste dann konkretere Mindestanforderungen und Risiken benennen. Insbesondere bei der Grundversorgung, den Grundrechten und Information der Bevölkerung müssen hohe Anforderungen an die Zuverlässigkeit gestellt werden. Die Piratenpartei schlägt beispielsweise vor, dass Personendaten grundsätzlich Ende-zu-Ende verschlüsselt werden müssen.<sup>1314</sup>

## § 22 Absatz 2

*Das Verzeichnis ist der Öffentlichkeit leicht zugänglich zu machen, insbesondere durch öffentliche Datennetze.*

Die Formulierung «leicht zugänglich [...] durch öffentliche Datennetze» lässt viel Interpretationsspielraum offen. Wir wünschen uns eine Umsetzung im Sinne von Open Data (vgl. Abschnitt «Fehlender Open Data Grundsatz»).

## § 27 Verweigerung oder Aufschub

Die Piratenpartei beider Basel kritisiert grundsätzlich jede Verweigerung beim Zugang zu Informationen. Insbesondere die «öffentliche Sicherheit», «Fabrikations- oder Geschäftsgeheimnisse» und «Urheberrechte» («Zensurheberrecht»<sup>15</sup>) sind zu allgemeine Formulierungen, die von Behörden zu leicht und ohne Angaben von weiteren Gründen geltend gemacht werden können, zulasten der Öffentlichkeit.

Aufschübe sollen befristet sein und sind einer Verweigerung immer vorzuziehen. Bei Anfragen von Medien (vgl. § 23 IDV) oder Nichtregierungs-Organisationen muss bei der Abwägung neben der zeitliche Dringlichkeit auch von einem erhöhten öffentlichen Interesse ausgegangen werden.

<sup>12</sup> [https://www.privatim.ch/wp-content/uploads/2019/12/privatim-Cloud-Papier\\_v2\\_1\\_20191217.pdf](https://www.privatim.ch/wp-content/uploads/2019/12/privatim-Cloud-Papier_v2_1_20191217.pdf)

<sup>13</sup> <https://www.piratenpartei.ch/2017/04/04/piratenpartei-fordert-verschluesselungspflicht/>

<sup>14</sup> <https://www.piratenpartei.ch/2019/08/18/die-piratenpartei-lehnt-den-aktuellen-entwurf-des-datenschutz-gesetzes-ab/>

<sup>15</sup> <https://fragdenstaat.de/blog/tag/zensurheberrecht/>

Behörden müssen unserer Ansicht nach immer transparent arbeiten und was aus öffentlichen Geldern finanziert wird, muss auch der Öffentlichkeit unentgeltlich zur Verfügung gestellt werden. Die Aufträge an Dritte müssen entsprechend ausgerichtet werden. Im digitalen Bereich unterstützen wir die Initiative «Public Money, Public Code»<sup>16</sup>.

Die «Zusicherung der Geheimhaltung» kann von Behörden gar nicht garantiert werden («Zusicherungsfalle»<sup>17</sup>) und eignet sich daher nicht als Begründung.

---

16 <https://publiccode.eu/de/>

17 Rudin, Beat (2014): Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Basel-Stadt (IDG), Seite 308