

Digitale Gesellschaft, CH-4000 Basel

Kanton Zürich
Direktion der Justiz und des Innern
Neumühlequai 10
8090 Zürich

Per E-Mail eingereicht über: <https://evernehmlassungen.zh.ch/de/totalrevisionidv/participant>

Basel, 20. August 2026

Stellungnahme zu den Verordnungen zum Gesetz über die Information und den Datenschutz des Kantons Zürich

Sehr geehrte Frau Regierungsrätin Fehr
Sehr geehrter Herr Henseler
Sehr geehrte Empfänger:innen

Am 4. Mai 2026 eröffnete der Regierungsrat des Kantons Zürich die Vernehmlassung über die drei Verordnungen zum Gesetz über die Information und den Datenschutz des Kantons Zürich (IDG), namentlich die Verordnung über die Information und den Datenschutz (IDV), die Verordnung über das Verzeichnis der algorithmischen Entscheidungssysteme (VAESV) und die Verordnung über den Datenkatalog und die offenen Behördendaten (DOBDV). Wir bedanken uns für die Möglichkeit zur Stellungnahme.

Die Digitale Gesellschaft ist eine gemeinnützige Organisation, die sich für Grund- und Menschenrechte, eine offene Wissenskultur, weitreichende Transparenz sowie Beteiligungsmöglichkeiten an gesellschaftlichen Entscheidungsprozessen einsetzt. Die Tätigkeit orientiert sich an den Bedürfnissen der Bürgerinnen und Konsumenten in der Schweiz und international. Das Ziel ist die Erhaltung und die Förderung einer freien, offenen und nachhaltigen Gesellschaft vor dem Hintergrund der Persönlichkeits- und Menschenrechte.

Gerne nehmen wir wie folgt Stellung:

1. Totalrevision IDV (Verordnung über die Information und den Datenschutz)

Allgemeine Anmerkung

Die Totalrevision der IDV konkretisiert das revidierte IDG in weiten Teilen sachgerecht und enthält verschiedene datenschutzrechtliche Sicherungen sowie transparenzfördernde Verbesserungen, was

ausdrücklich zu begrüßen ist. Einzelne Bestimmungen entsprechen jedoch dem durch höherrangiges Recht vorgegebenen datenschutzrechtlichen Rahmen nicht und schwächen die Stellung der betroffenen Personen unnötig ab. Zur Rechtfertigung einzelner Regelungen wird teilweise auf bereits bestehende Vollzugsdefizite verwiesen. Diese Argumentation überzeugt jedoch nicht: Eine mangelhafte Vollzugspraxis darf nicht als Rechtfertigung für herabgesetzte datenschutzrechtliche Standards dienen.

Ausserdem zieht sich durch alle drei Verordnungen die Problematik, dass nicht klar wird, welcher datenschutzrechtliche Standard ihnen zugrunde gelegt wird. Wiederholt wird auf das Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (SEV 108+) des Europarates verwiesen, um die Übereinstimmung einzelner Regelungen mit dessen Vorgaben zu begründen. Gleichzeitig enthält etwa der VE-IDV eine Bestimmung, die diesen Anforderungen gerade nicht entspricht, ohne dass die Abweichung näher begründet wird. Da das SEV 108+ ein von der Schweiz ratifizierter völkerrechtlicher Vertrag ist, sollte der darin vorgesehene Datenschutzstandard (ungeachtet des Umstands, dass ihn noch nicht alle Vertragsstaaten ratifiziert haben) konsequent eingehalten werden.

§ 7

Die Bestimmung bezweckt das Schaffen von mehr Transparenz, indem sie das Verzeichnis der öffentlichen Informationsbestände gemäss § 14 Abs. 2 IDG konkretisiert. Insofern ist die allgemeine Konkretisierung des Begriffes "Informationsbestand" in Abs. 1 zu begrüßen. Abs. 3 enthält zusätzliche Anforderungen an die Angaben im Verzeichnis bei Informationsbeständen, die Personendaten enthalten - die Unterscheidung sowie verschärfte Kriterien sind sinnvoll. Der gemäss den Erläuterungen "bewusste" Verzicht auf einerseits die Angabe der Empfängerstaaten sowie andererseits der Rechtsgrundlage, die eine grenzüberschreitende Bekanntgabe erlaubt (§ 41 IDG), überzeugt jedoch nicht.

In den Erläuterungen wird vorgebracht, dass die Empfängerstaaten regelmässig nur schwer zu eruieren seien und dass damit ohnehin schon "Vollzugsdefizite" bestünden. Sofern nun auch die Angabe von Empfängerstaaten verlangt würde, verschärft dies die bestehende Problematik. Aus einer mangelhaften Praxis darf aber nicht einfach abgeleitet werden, dass das Problem ohnehin bestünde und deshalb künftig gelockerte Anforderungen zulässig seien.

Im Bund gibt es eine explizite entsprechende Pflicht zur Angabe der Empfängerstaaten (Art. 12 Abs. 2 lit. g DSG), ebenso im EU-Recht (Richtlinie 2016/680). Mit der beabsichtigten Regelung im VE-IDV werden somit die weithin anerkannten datenschutzrechtlichen Standards unterschritten. Mit Blick auf die Grundrechte erscheint ohnehin als fraglich, ob der Verzicht auf diese Informationen im Verzeichnis rechtskonform ist. Für Betroffene ist damit nämlich (abstrakt) nicht nachvollziehbar, wohin ihre Daten gelangen (können), ausserdem bleibt für sie unklar, gestützt auf welche Rechtsgrundlage die grenzüberschreitenden Bekanntgaben erfolgen. Diese Regelung widerspricht denn auch klar dem eigentlichen Zweck des IDG (§ 1 Abs. 2 IDG): Die Ausgestaltung macht das Handeln der öffentlichen Organe keineswegs transparent (wie in § 1 Abs. 2 lit. a IDG geboten) und schützt die Grundrechte nicht (§ 1 Abs. 2 lit. c IDG). Damit vollzieht die Verordnung nicht den gesetzlichen Rahmen, sondern unterläuft diesen.

Zudem erklären die Erläuterungen – ebenfalls unter Verweis auf die bestehenden Vollzugsdefizite –, man verzichte im VE-IDV bewusst darauf, Hinweise auf allfällige Auftragsdatenbearbeitungen als zwingenden Inhalt des Verzeichnisses aufzunehmen. Dies, obwohl das "Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten" des Europarates (SEV 108+) diese Vorgabe nennt. Das SEV 108+ wurde von der Schweiz bereits ratifiziert und soll somit konsequent beachtet werden.

Forderung: Im Verzeichnis sind die Empfängerstaaten, die Rechtsgrundlage gem. § 41 IDG sowie Hinweise auf allfällige Auftragsdatenbearbeitungen aufzunehmen.

§ 12

Die zehntägige Frist in Abs. 4, nach Ablauf derer ein Gesuch als zurückgezogen gilt, sofern die gesuchstellende Person nicht die für die Identifizierung der verlangten Informationen zusätzlich erforderlichen Angaben gemacht hat, ist sehr kurz. Das Stellen von Gesuchen nach dem Öffentlichkeitsprinzip soll möglichst niederschwellig und auch ohne juristische Kenntnisse möglich sein, Aufwand und Risiko für die Gesuchstellenden sollen zudem möglichst klein gehalten werden. Somit wäre eine längere Frist wünschenswert.

Forderung: Die Frist ist von zehn auf dreissig Tage anzuheben.

§ 21

§ 21 Abs. 3 VE-IDV steht im Widerspruch zu § 24 Abs. 3 IDG: Dieser sieht vor, dass die am Verfahren beteiligten Personen auf eine Teilnahme am Schlichtungsverfahren verzichten können. Damit soll sichergestellt werden, dass ein Schlichtungsverfahren auch tatsächlich durchgeführt wird.

§ 21 Abs. 3 VE-IDV sieht jedoch vor, dass das Verfahren abgeschrieben wird, wenn die gesuchstellende Person nicht an einer Schlichtungsverhandlung teilnimmt und sich nicht vertreten lässt. Die Verordnungsbestimmung ist nicht vom Gesetz gedeckt und stellt damit eine unzulässige verfahrensrechtliche Einschränkung dar.

Forderung: Abs. 3 ist ersatzlos zu streichen.

§ 26

Grundsätzlich ist eine Liste, die ein hohes Risiko für Grundrechtseingriffe bzw. -verletzungen aufzeigt und die Vorabkontrolle, die dadurch ausgelöst wird, sehr zu begrüßen. Positiv hervorzuheben ist der nicht abschliessende Charakter der Liste, da hiermit anerkannt wird, dass weitere Grundrechtsrisiken bestehen. Die beispielhafte Aufzählung könnte jedoch um eine weitere litera ergänzt werden, die festhält, dass auch dann ein hohes Risiko für die Grundrechte vorliegt, wenn aufgrund kleiner Fallzahlen oder kleiner betroffener Personengruppen die Re-Identifikation einzelner Personen möglich oder erheblich erleichtert wird.

Forderung: Ergänzung der beispielhaften Aufzählung um Fälle, in denen aufgrund kleiner Fallzahlen oder kleiner Personengruppen Rückschlüsse auf einzelne Personen möglich sind.

§ 27

Die Norm enthält einen offensichtlichen Fallfehler ("Das öffentlichen Organs teilt der oder dem..."). Dies spricht nicht für eine sorgfältige Gesetzgebung und ist insofern bedauerlich.

Forderung: Der Fallfehler ist zu beheben.

§ 31

Die Bestimmung regelt die Bekanntgabe von Personendaten zu nicht personenbezogenen Zwecken und orientiert sich am bislang gültigen § 21 Abs. 1 IDV. Dieser verweist jedoch in das aIDG, das vorsah, dass die Empfängerin oder der Empfänger nachzuweisen hat, dass die Personendaten anonymisiert werden, dass aus den Auswertungen keine Rückschlüsse auf betroffene Personen möglich sind und dass die ursprünglichen Personendaten nach der Auswertung vernichtet werden (§18 Abs. 2 aIDG). Das neue IDG kennt keine entsprechende Pflicht, der VE-IDV ebenso. Dies ist jedoch problematisch: Es muss nach wie vor sichergestellt werden, dass Personen nicht mehr bestimmbar sein können bei der Bekanntgabe von Personendaten zu nicht personenbezogenen Zwecken. Dies ergibt sich denn auch bereits aus dem höherrangigen Recht (Art. 8 EMRK sowie Art. 13 Abs. 2 BV). Der Verzicht auf die Nennung dieser notwendigen Sicherungen führt folglich auch nicht dazu, dass die materielle Pflicht entfiel. Der Rechtssicherheit halber soll jedoch in der IDV eine entsprechende Bestimmung enthalten sein.

Forderung: Die in § 18 Abs. 2 aIDG vorgesehenen datenschutzrechtlichen Sicherungen sind in § 31 VE-IDV zu übernehmen.

§ 36

§ 36 VE-IDV regelt die Kommunikation zwischen der oder dem Beauftragten für das Öffentlichkeitsprinzip und den Datenschutz und den öffentlichen Organen. Für Angelegenheiten von allgemeiner Bedeutung oder besonderer Tragweite sieht die Bestimmung vor, dass die Kommunikation auf dem Dienstweg über die Direktion erfolgt. Dies steht im Spannungsverhältnis zur gesetzlich gewährleisteten Unabhängigkeit der oder des Beauftragten. Kommunikationsvorgaben über die beaufsichtigten Organe beeinträchtigen die institutionelle Unabhängigkeit und schaffen unnötige Abhängigkeiten.

Forderung: § 36 Abs. 2 und 3 VE-IDV sind ersatzlos zu streichen. In § 36 Abs. 1 ist der Satz "In Angelegenheiten von allgemeiner Bedeutung oder besonderer Tragweite erfolgt die Kommunikation auf dem Dienstweg über die Direktion." zu streichen.

2. Erlass VAESV (Verordnung über das Verzeichnis der algorithmischen Entscheidungssysteme)

Allgemeine Anmerkung

Die Einführung eines Verzeichnisses algorithmischer Entscheidungssysteme (AES) ist ausdrücklich zu begrüssen und stellt einen wichtigen Schritt zur Verbesserung der Transparenz staatlicher Datenbearbeitungen dar. Der vorliegende Verordnungsentwurf schöpft das mit § 14 Abs. 3 IDG

verfolgte Transparenzziel jedoch noch nicht vollständig aus. Insbesondere erscheint die dem Verordnungsentwurf zugrunde gelegte Definition von AES zu eng, der Umfang der zu veröffentlichenden Informationen teilweise unzureichend und die Ausnahmen vom Grundsatz der Veröffentlichung zu weit gefasst.

§ 1

Die dem VE-VAESV zugrunde gelegte AES-Definition der Staatskanzlei verengt den gesetzlichen Begriff des algorithmischen Entscheidungssystems unzulässigerweise auf KI-Systeme. Dies steht im Widerspruch zum gesetzlichen Wortlaut: § 14 Abs. 3 IDG spricht allgemein von "algorithmischen Entscheidungssystemen", die sich auf die Grundrechte von Personen auswirken können.

Die Definition der Staatskanzlei ist auch darüber hinaus problematisch: Einerseits ist der Begriff "KI-System" unpräzise, da er technisch nicht eindeutig definiert ist und unterschiedlich verstanden und verwendet wird. Im allgemeinen Sprachgebrauch werden unter "KI-Systemen" regelmässig Modelle verstanden, die auf Machine Learning beruhen oder hochkomplexe neuronale Netzwerke verwenden. Nicht (klar) erfasst sind von diesem allgemeinen Verständnis hingegen algorithmische Entscheidungssysteme wie regelbasierte Modelle oder automatisierte Systeme zur Risikobewertung bzw. algorithmische Prognosesysteme.

Gerade letztere können jedoch in hohem Masse intransparent und für die Betroffenen nicht nachvollziehbar sein, wie etwa das System [COMPAS](#) in den USA eindrucksvoll gezeigt hat. Auch können entsprechende Systeme schwer diskriminierend sein, wie der Skandal um das Risikobewertungssystem [SyRI](#) in den Niederlanden deutlich machte. Somit müssen derartige Systeme ebenfalls vom Wortlaut von § 14 Abs. 3 IDG bzw. § 1 VE-VAESV erfasst sein. Weiter ist die Gleichsetzung von AES mit KI-Systemen begrifflich unzutreffend: Regelbasierte Modelle und algorithmische Prognosesysteme sind ebenfalls algorithmische Systeme, die Entscheide treffen oder massgeblich vorbereiten. Diese Tatsache ist umso erheblicher, als der Grossteil der heute von öffentlichen Verwaltungen zur Entscheidungsfindung eingesetzten algorithmischen Systeme regelbasiert ist.

Zwar stellen sich bei klassischen KI-Systemen Transparenzprobleme aufgrund des "Black-Box-Phänomens" in verschärfter Form – dies rechtfertigt es jedoch nicht, andere algorithmische Entscheidungssysteme von der Definition auszuklammern.

Schliesslich birgt eine zu enge Definition die Gefahr, dass öffentliche Organe gezielt algorithmische Entscheidungssysteme einsetzen, die keine "KI" im Sinne der verwendeten Definition darstellen, um der Registerpflicht zu entgehen. Dadurch würde der Zweck des AES-Verzeichnisses, Transparenz über den Einsatz algorithmischer Entscheidungssysteme zu schaffen, teilweise unterlaufen.

Nicht zuletzt hat auch der Regierungsrat das erhebliche Interesse an einer Offenlegung der Verwendung von algorithmischen Entscheidungssystemen, die einen Einfluss auf die Grundrechte haben können, anerkannt, und zwar "unabhängig davon, ob es sich um komplexe Systeme, die mit Mustererkennung arbeiten, handelt oder um einfache Systeme, die nach festen Regeln ohne Entscheidungsspielraum handeln" ([erläuternder Bericht zum IDG](#), S. 64).

Forderung: Es ist ein separater Paragraph in die Verordnung aufzunehmen, der eine Legaldefinition von AES enthält, die sich nicht auf "KI-Systeme" beschränkt. Die Legaldefinition muss sämtliche algorithmischen Entscheidungssysteme erfassen, die Entscheide eigenständig treffen oder massgeblich vorbereiten und sich auf die Grundrechte von Personen auswirken können.

§ 2

§ 2 Abs. 3 VE-VAESV regelt zwar die Zuständigkeit der weiteren öffentlichen Organe zur Führung ihrer AES-Verzeichnisse, enthält jedoch keine Bestimmung zur zentralen Auffindbarkeit dieser Verzeichnisse.

Forderung: Um den mit § 14 Abs. 3 IDG verfolgten Transparenzzweck wirksam zu gewährleisten, sollte die Staatskanzlei dazu verpflichtet werden, eine zentrale, öffentlich zugängliche Übersicht sämtlicher AES-Verzeichnisse zu veröffentlichen.

§ 3

Die in § 3 VE-VAESV vorgesehenen Angaben genügen dem Transparenzzweck von § 14 Abs. 3 IDG nur teilweise. Damit das AES-Verzeichnis einen echten Mehrwert für die Öffentlichkeit schafft, müssen die erfassten Informationen aussagekräftig, verständlich und zwischen den einzelnen öffentlichen Organen vergleichbar sein. Die Angaben sollten daher soweit möglich standardisiert erfasst und in nachvollziehbare Informationskategorien gegliedert werden. Sinnvoll erscheinen die Kategorien "Informationen zur verantwortlichen Institution", "Informationen zum AES selbst" und zur "Kritikalität", also der Risikobewertung des jeweiligen AES. Im aktuellen Vorentwurf fehlen verschiedene Informationen, die für eine sachgerechte Einordnung des Einsatzes algorithmischer Entscheidungssysteme wesentlich sind.

Die drei genannten Kategorien sollten folgende Punkte enthalten:

- Informationen zur verantwortlichen Institution
 - Name der verantwortlichen Institution/Stelle
 - Art der Institution
 - Weiterführende Angaben zur Institution
 - Kontaktangabe der Institution
 - Webseite der Institution
- Informationen zum AES
 - Name des AES
 - Beschreibung des AES
 - Zweck des AES
 - Information dazu, ob das AES einen Entscheid vollautomatisiert trifft oder ob es einen menschlichen Entscheid lediglich massgeblich vorbereitet
 - Rechtsgrundlage für den Einsatz des AES (wurde gemäss den Erläuterungen bewusst nicht in den VE aufgenommen, weiterführende Kritik dazu s. u.)
 - Einsatzfelder des AES
 - Webseite zum AES
 - Technologiefelder des AES

- Wertschöpfungsbereiche des AES
- Genutzte Informationen und Betriebslogik des AES
- ev. unterteilen: Offenlegung der verwendeten
 - a) Trainingsdaten
 - b) Eingabedaten
- ev. auch: Ort der Speicherung der verwendeten Daten sowie Angaben dazu, ob die Daten für das weitere Training und die Optimierung der Systeme (oder der KI-Produkte der Hersteller) verwendet werden
- Inbetriebnahme des AES
- Informationen zur Kritikalität des AES
 - Grundrechtliche Folgenabschätzung (inkl. identifizierter Risiken und Massnahmen zur Bewältigung der Risiken, Zeitpunkt der Durchführung)
 - Datenschutzfolgenabschätzung

Die Erläuterungen begründen den Verzicht auf die Angabe der Rechtsgrundlage unter anderem damit, dass sich die Grundlage für den Einsatz eines AES häufig aus den gesetzlichen Aufgaben des jeweiligen öffentlichen Organs ableite und daher oftmals keine ausdrückliche Rechtsgrundlage bestehe. Diese Begründung überzeugt nicht. Gerade im grundrechtssensiblen Bereich algorithmischer Entscheidungssysteme stellt die Angabe der Rechtsgrundlage eine zentrale Information dar. Dies gilt unabhängig davon, ob die Rechtsgrundlage ausdrücklich den Einsatz des AES regelt oder sich aus einer gesetzlichen Aufgabenzuweisung ergibt. Die Öffentlichkeit hat ein berechtigtes Interesse daran, nachvollziehen zu können, auf welche gesetzliche Grundlage der Einsatz eines algorithmischen Entscheidungssystems gestützt wird. Dies gilt umso mehr, als der Einsatz von AES in der öffentlichen Verwaltung politisch und gesellschaftlich besonders sensibel ist und sich der Bereich derzeit dynamisch entwickelt. Schliesslich kann der Umstand, dass für den Einsatz eines AES teilweise keine ausdrückliche gesetzliche Grundlage besteht, nicht als Begründung dafür dienen, auf die Angabe der Rechtsgrundlage zu verzichten. Eine mangelhafte und rechtsstaatlich fragwürdige Praxis darf nicht als logischer Ausgangspunkt für gelockerte Anforderungen gelten. Die vorgeschlagene Struktur und die aufgeführten Ergänzungen orientieren sich an den Empfehlungen des 2025 veröffentlichten Policy Papers ["Ein verbindliches KI-Transparenzregister für Deutschland: Empfehlungen für mehr Verantwortung, Vertrauen und Teilhabe im digitalen Staat"](#) der NGO AlgorithmWatch.

Forderung: § 3 VE-VAESV ist dahingehend zu ergänzen, dass die zu veröffentlichenden Angaben möglichst standardisiert und in klaren Informationskategorien erfasst werden. Das AES-Verzeichnis soll die genannten Punkte erfassen. Zudem soll § 3 VE-VAESV festhalten, dass für jedes im AES-Verzeichnis erfasste algorithmische Entscheidungssystem die gesetzliche Grundlage seines Einsatzes anzugeben ist.

§ 4

Die Pflicht zur Überprüfung und Aktualisierung der Angaben im AES-Verzeichnis ist sinnvoll und zu begrüssen. Auch die Kennzeichnungspflicht für nicht mehr eingesetzte AES ist zu begrüssen. Damit das staatliche Handeln nachvollziehbar bleibt, ist es jedoch zentral, dass die Systeme nicht bereits nach einem Jahr ohne Einsatz entfernt werden. Es wäre somit sinnvoll, dass das Verzeichnis um einen Abschnitt "Nicht mehr verwendete AES" ergänzt wird.

Forderung: Abs. 3 ist dahingehend anzupassen, dass die AES, die ein Jahr lang nicht verwendet wurden, in den neu zu schaffenden Abschnitt "Nicht mehr verwendete AES" aufgenommen werden.

§ 5

Die Ausnahme des Grundsatzes der Veröffentlichung ist nicht unproblematisch: Das vorgebrachte Geheimhaltungsinteresse steht in starkem Widerspruch zur Transparenzfunktion des IDG und den dazugehörigen Verordnungen.

Das entscheidende Kriterium für die Nichtveröffentlichung eines AES ist gemäss Abs. 1 die Zweckvereitelung: AES sind nur insoweit in das AES-Verzeichnis aufzunehmen, als dadurch deren Zweck nicht vereitelt wird. Da die Nichtbekanntmachung zu einem erheblichen Transparenzdefizit führt, darf eine derartige Ausnahme – wenn überhaupt – nur unter engen Voraussetzungen gewährt werden. Vor allem muss nachvollziehbar sein, welche Interessen eine Ausnahme rechtfertigen können. Aus dem Vorentwurf wird jedoch keineswegs klar, unter welchen Voraussetzungen davon auszugehen ist, dass bereits die Kenntnisnahme von der Existenz eines AES zu einer Zweckvereitelung führen würde. Damit mangelt es dem Vorentwurf an der erforderlichen Transparenz hinsichtlich der Voraussetzungen der Ausnahme. Ohne eine entsprechende Konkretisierung erscheint eine derart weitgehende Ausnahme vom Grundsatz der Veröffentlichung nicht gerechtfertigt und als zu weitgehend.

Dies gilt umso mehr, als es sich bei algorithmischen Datenbearbeitungen regelmässig um schwerwiegende Grundrechtseingriffe handelt, die systembedingt oftmals ohnehin mit einer verminderten Transparenz einhergehen und damit eine erhöhte Gefahr für Grundrechte darstellen. Abgesehen davon braucht es auch für Datenbearbeitungen im Bereich staatlicher Geheimhaltungsinteressen jeweils eine ausreichende gesetzliche Grundlage. Damit ist eine absolute Geheimhaltung ohnehin nicht möglich.

Forderung: Es ist klar darzulegen, unter welchen engen Voraussetzungen eine Ausnahme vom Grundsatz der Veröffentlichung zulässig sein soll und welche Interessen eine Ausnahme rechtfertigen können.

3. Erlass DOBDV (Verordnung über den Datenkatalog und die offenen Behördendaten)

Allgemeine Anmerkung

Die DOBDV setzt die mit der Totalrevision des IDG angestrebte Förderung von Transparenz und Nachvollziehbarkeit staatlichen Handelns grundsätzlich überzeugend um. Insbesondere die Einführung des Datenkatalogs und die systematische Erfassung von Informationsbeständen schaffen eine wichtige Grundlage für einen transparenten Umgang mit behördlichen Informationen. Ebenfalls ausdrücklich zu begrüssen ist die Förderung offener Behördendaten sowie die Verpflichtung der öffentlichen Organe, zu

prüfen und zu dokumentieren, ob Informationen als offene Behördendaten veröffentlicht werden können. Positiv hervorzuheben ist zudem die vorgesehene Erfassung von Metadaten, welche die Auffindbarkeit und Nutzbarkeit der Informationen verbessert. Die nachfolgenden Kritikpunkte sind daher nur punktuell, während die grundsätzliche Stossrichtung überzeugt.

§ 6

§ 6 Abs. 2 regelt die Bekanntgabe von mehrfach genutzten Personendaten und hält fest, dass die Zulässigkeit einer Bekanntgabe vorgängig aufgrund der Angaben des empfangenden Organs geprüft werden muss. Für die Prüfung ist das zuständige Organ verantwortlich. Die Zulässigkeit einer Bekanntgabe bzw. die erforderlichen Angaben werden in der Verordnung allerdings nicht genannt, während die Erläuterungen erklären, dass auch die Rechtsgrundlage vom empfangenden Organ anzugeben ist.

Wenn § 6 die Voraussetzungen für die Prüfung einer Datenbekanntgabe bei mehrfachnutzbaren Personendaten konkretisieren soll, müssen die erforderlichen Angaben aus der Verordnung selbst ersichtlich sein. Die Verordnung legt zwar eine Prüfungspflicht fest, bestimmt jedoch nicht, welche Angaben dem verantwortlichen Organ für diese Prüfung vorliegen müssen. Dass wesentliche Verfahrensanforderungen lediglich in den Erläuterungen erwähnt werden, ohne im normativen Text festgelegt zu sein, ist problematisch. Die Voraussetzungen für die Prüfung der Zulässigkeit der Bekanntgabe sollten daher in der Verordnung ausformuliert sein. Insbesondere muss klar sein, dass das empfangende Organ verpflichtet ist, die Rechtsgrundlage sowie die beabsichtigte Bearbeitung, die den Erhalt der Personendaten erlauben, anzugeben.

Forderung: § 6 ist entsprechend zu ergänzen, sodass der zwingende Inhalt der Angaben des empfangenden Organs ausdrücklich geregelt wird.

§ 8

Die Bestimmung regelt die Ausnahme vom Grundsatz des Datenkatalogs: Sie legt fest, unter welchen Voraussetzungen ein Informationsbestand nicht in den Datenkatalog aufgenommen werden muss. Die Erläuterungen erklären, dass die Ausnahmeregelung eng zu verstehen sei, da der Datenkatalog eine möglichst weitgehende Transparenz beabsichtige: Vom Katalog dürften lediglich Informationsbestände ausgenommen werden, deren Existenz der breiten Öffentlichkeit nicht bekannt sein soll.

Die sehr offen formulierten Geheimhaltungsinteressen in Abs. 2 ("insbesondere die öffentliche Sicherheit und Ordnung") stehen dem angestrebten Transparenzziel entgegen und verdeutlichen entgegen den Erläuterungen keineswegs, dass nur "ganz bestimmte Interessen" eine Ausnahme rechtfertigen sollen. Dazu kommt, dass die Erläuterungen nicht erklären, inwiefern Ausnahmen überhaupt notwendig sein können, um berechnigte Geheimhaltungsinteressen zu wahren. Auch wird nicht weiter konkretisiert, was unter den berechtigten Geheimhaltungsinteressen zu verstehen ist – die verwendeten Begriffe der öffentlichen Sicherheit und Ordnung helfen hier kaum weiter.

Forderung: Es ist klar darzulegen, unter welchen engen Voraussetzungen eine Ausnahme vom Grundsatz der Aufnahme in den Datenkatalog zulässig sein soll. Diese Voraussetzungen sind in der Verordnung selbst zu konkretisieren.

Schlussbemerkung

Wir beschränken uns in dieser Stellungnahme auf unsere Kernanliegen. Der Verzicht auf umfassende allgemeine Anmerkungen oder auf Anmerkungen zu einzelnen Artikeln bedeutet keine Zustimmung der Digitalen Gesellschaft.

Freundliche Grüsse



Rahel Estermann
Co-Geschäftsleiterin



Luka Studer
Legal Counsel