4. Juni 2025
Version 2.0

DIGITALE GESELLSCHAFT

DATENSCHUTZ-KONZEPT

Das Datenschutz-Konzept setzt neue Massstäbe für einen zeitgemässen und effektiven Datenschutz. Die aktualisierte Version baut auf dem wegweisenden Ansatz auf, Datenschutz aus der Verantwortung der Betroffenen herauszunehmen und stattdessen klare Rahmenbedingungen für die datenverarbeitenden Stellen festzulegen.

DIGITALE GESELLSCHAFT / CH-4000 BASEL
OFFICE@DIGITALE-GESELLSCHAFT.CH / DIGITALE-GESELLSCHAFT.CH

1 EINLEITUNG

Die fortschreitende Digitalisierung und die rasante Weiterentwicklung von Technologien bringen sowohl Chancen als auch Gefahren mit sich. Insbesondere die Vernetzung von grossen Datenbeständen sowie der Einsatz von künstlicher Intelligenz tangieren die Persönlichkeitsrechte der Menschen. Der Digital Radar Schweiz 2024 hat jüngst gezeigt, dass die Gefahren aufgrund der persönlichen Nutzung von digitalen Technologien signifikant höher bewertet werden als in früheren Umfragen. Dabei bezeichneten die Befragten «Datenschutz/IT-Sicherheit» und «Überwachung durch Technologien» als die wichtigsten Nachteile digitaler Technologien.

Viele Menschen fühlen sich durch die Digitalisierung überfordert. Bestärkt wird das daraus entstehende Unwohlsein durch die fast wöchentlich zu lesenden Berichte über Datenverluste. Dies schwächt das Vertrauen in den Umgang mit Daten. Das Vertrauen in der Bevölkerung ist jedoch von entscheidender Bedeutung, sollen neue Möglichkeiten der digitalen Demokratie und für E-Government, aber auch neue digitale Geschäftsmodelle geschaffen werden. Dasselbe gilt für sogenannte Datenräume, in denen eine «Sekundärnutzung» von Personendaten über den ursprünglichen Zweck hinaus möglich werden soll.

Um das nötige Vertrauen zu schaffen, braucht es einen sorgsamen Umgang mit Daten, der auf einem zielgerichteten und wirksamen Datenschutz basiert. Datenschutz und Datennutzung sind daher kein Widerspruch – im Gegenteil: sie bedingen einander.

2 VORAUSSETZUNGEN DER DATENBEARBEITUNG NACH DEM DATENSCHUTZGESETZ

Zweck des Datenschutzgesetzes ist laut Art. 1 DSG der «Schutz der Persönlichkeit und der Grundrechte der natürlichen Personen, über die Daten bearbeitet werden». Dies ist eine sehr offene und allgemeine Formulierung, und es bleibt unklar, was konkret geschützt werden soll.

Die Voraussetzungen für eine rechtmässige Datenbearbeitung sind in Art. 6 (i.V.m. Art. 31) DSG festgehalten. Die Bearbeitung von Personendaten muss rechtmässig, transparent, nach Treu und Glauben sowie verhältnismässig erfolgen. Zudem ist sie an den Grundsatz der Zweckbindung gebunden. Verantwortliche sind überdies verpflichtet, die Richtigkeit der Daten sicherzustellen. Darüber hinaus enthält das DSG Bestimmungen zur Anonymisierung von Daten, um Persönlichkeitsrechte zu wahren. Anonymisierte Daten unterliegen in der Regel nicht den Anforderungen des Datenschutzgesetzes, solange der Bezug zur betroffenen Person nicht wiederhergestellt werden kann. Jedoch zeigt sich in der Praxis, dass eine tatsächliche Anonymität oft schwer zu gewährleisten ist.

Eine Datenbearbeitung durch Private ist gemäss Art. 31 DSG nur zulässig, wenn sie auf der Einwilligung der betroffenen Person, einem überwiegenden öffentlichen oder privaten Interesse oder einer gesetzlichen Grundlage beruht. Erfolgt die Datenbearbeitung hingegen durch ein Bundesorgan, so bedarf es zur Rechtmässigkeit gemäss Art. 34 in jedem Fall einer gesetzlichen Grundlage. Folglich kann eine Bearbeitung von (besonders schützenswerten) Personendaten durch gesetzliche Grundlage oder überwiegendes privates oder öffentliches Interesse gerechtfertigt sein, ohne dass die betroffene Person jemals davon erfährt oder eingewilligt hat.

3 DIE GRENZEN DES DATENSCHUTZES IN DER SCHWEIZ

Beim Datenschutzgesetz handelt es sich um eine Konkretisierung des verfassungsmässigen Persönlichkeitsschutzes. Gemäss Art. 13 Abs. 2 der Bundesverfassung hat jede Person Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten. Diese Einschränkung des Wortlauts auf den Missbrauch der persönlichen Daten wird dem Schutzgedanken nicht gerecht und greift entsprechend zu kurz (vgl. Stämpflis Handkommentar zum Datenschutzgesetz).

In der Praxis hat sich hinsichtlich Art. 13 Abs. 2 BV auch der Begriff des Rechts auf informationelle Selbstbestimmung etabliert. Dieses bezeichnet das Recht der Individuen, grundsätzlich selbst über die Preisgabe und Verwendung ihrer persönlichen Daten bestimmen zu können. Das klingt eingängig, ist gesetzlich aber nur schwach abgestützt und lässt sich in der Praxis nur limitiert einfordern. Überwiegende Interessen der Datenbearbeiter:innen oder gesetzliche Pflichten schränken es deutlich ein. Weiter gibt es die Kritik, als individuelles Recht die Verantwortung den Betroffenen zu überlassen; sei es, sich durch Cookie-Banner zu klicken, die richtigen Datenschutz-Einstellungen zu finden oder sich gegen übergriffige Praktiken zu wehren. Überdies betrifft Datenschutz nicht nur die einzelnen Personen, die ihre Daten preisgeben, sondern auch die Gesellschaft als Ganzes.

Ausgangspunkt des schweizerischen Datenschutzrechts ist nach unserem Verständnis das Recht auf Achtung des Privatlebens gemäss Art. 8 der Europäischen Menschenrechtskonvention (EMRK). Weder das angesprochene Missbrauchsparadigma noch das Recht auf informationelle Selbstbestimmung vermögen dieses Recht auf Privatleben umfassend zu gewährleisten.

Angesichts dieser Defizite ist es erforderlich, den Datenschutz zu überdenken und ein neues Konzept als Grundlage zu entwickeln. Datenschutz ist kein Selbstzweck. Dafür ist es zunächst notwendig, klar zu definieren, wovor das Datenschutzrecht Menschen tatsächlich schützen soll. Diese Schutzziele und das daraus resultierende Konzept sollen sicherstellen, dass den Individuen und der Gesellschaft als Ganzes aus den Datenbearbeitungen keine Nachteile erwachsen. Gleichzeitig sollen sie dafür sorgen, dass der Raum für Innovation offen bleibt.

Ein wirksamer und umfassender Datenschutz muss eine Selbstverständlichkeit sein, auf die sich die Leute verlassen können – ohne selber aktiv werden zu müssen.

4 SCHUTZZIELE

Ausgehend von der Kritik am zu wenig spezifischen Zweck des Datenschutzgesetzes und seinem unklaren Schutzbereich müssen konkrete Schutzziele formuliert werden. Es ergeben sich folgende sechs Schutzziele:

4.1 Schutz vor Manipulation

Mit dem Schutz vor Manipulation sollen die individuelle Entscheidungsfreiheit und die Willensbildung geschützt werden.

Als Manipulation zu verstehen ist die absichtliche, gezielte und in der Regel verdeckte Einflussnahme auf die Entscheidung einer anderen Person, um deren Selbstkontrolle und Entscheidungskraft zu unterlaufen. Die Manipulation kann zu einem Nachteil für die betroffene Person führen. Sie zielt, unter Ausnützung menschlicher Schwächen, auf eine Steuerung des Verhaltens von Individuen oder Gruppen.

4.2 Schutz vor Diskriminierung

Datenbearbeitungen dürfen nicht diskriminierend sein. Eine Diskriminierung gemäss Art. 8 Abs. 2 BV liegt vor, wenn eine Person rassistisch[1.] oder aufgrund geschützter Merkmale wie Herkunft, Geschlecht, Alter, Sprache, soziale Stellung, Lebensform, religiöse, weltanschauliche oder politische Überzeugung oder körperliche, geistige oder psychische Behinderung ohne qualifizierte Rechtfertigung unterschiedlich behandelt wird.

Regulierungen zum Schutz vor Diskriminierung finden sich vereinzelt in Gesetzen wie im Strafrecht (Art. 261bis StGB), im Gleichstellungsgesetz (GlG) oder im Behindertengleichstellungsgesetz (BehiG). Diese Bestimmungen haben allerdings nicht direkt die Diskriminierung durch Datenbearbeitungen zum Gegenstand. Der zivilrechtliche Persönlichkeitsschutz schützt vor Persönlichkeitsverletzungen (Art. 28 ff. ZGB), doch steht Diskriminierung nicht im Zentrum. Deshalb vermögen bestehende Regelungen nicht genügend vor Diskriminierung durch Datenbearbeitungen zu schützen.

4.3 Schutz vor Überwachung und Wahrung der Anonymität

Mit dem Schutz vor Überwachung soll sichergestellt werden, dass die persönliche Freiheit und die Persönlichkeitsentwicklung (Art. 10 Abs. 2 BV), die freie Meinungsäusserung (Art. 16 BV) sowie weitere Grundrechte wie insbesondere die Versammlungsfreiheit (Art. 22 BV) und die Privatsphäre (Art. 13 BV) gewährleistet sind. Entsprechend ist wichtig, dass bei der Wahrnehmung der Grundrechte keine Abschreckungseffekte («chilling effects») wirken.

Die Wahrung der Anonymität gewährleistet die Bewegungsfreiheit, um sich im öffentlichen Raum grundsätzlich anonym bewegen und verhalten zu können.

Die Wahrung der Anonymität ist ebenso von zentraler Bedeutung, wenn es darum geht, Grundrechte im digitalen Raum wahrzunehmen. Anonymität im Internet soll uns vor unerwünschter Überwachung schützen. In repressiven Staaten soll sie den Austausch von Informationen unter gefährlichen Bedingungen ermöglichen. Sie gewährleistet persönliche Freiheit(en) und schützt vor Diskriminierung. Ausserdem bietet Anonymität Schutz vor unerwünschter Überwachung und Datensammlung, was besonders im digitalen Zeitalter ein wichtiger Aspekt des Datenschutzes ist.

Anonymisierung kann problematische Dynamiken wie Hassrede und Radikalisierung zwar allenfalls begünstigen. Untersuchungen zeigen jedoch, dass diese Dynamiken nicht durch Anonymität entstehen, sondern auch gleichermassen unter Klarnamen stattfinden. Zudem gibt es wirksame Massnahmen, wie die Gegenrede, um diese Dynamiken zu bekämpfen und gleichzeitig die Anonymität zu wahren.

4.4 Schutz vor Beeinträchtigung der Gesundheit sowie der Lebens- und Entwicklungschancen

Mit dem Schutz vor Beeinträchtigung der psychischen und physischen Gesundheit sowie der Lebens- und Entwicklungschancen soll sichergestellt werden, dass Menschen nicht durch eine (falsche) Beurteilung insbesondere durch Automated Decision-Making Systeme (ADMS, künstliche Intelligenz) geschädigt werden. Dies beinhaltet das Recht auf eine (Neu-)Beurteilung durch ein Individuum sowie das Recht auf zusätzliche Schutzmassnahmen wie höhere Sorgfaltspflichten oder eine Zertifizierung.

4.5 Schutz vor Stigmatisierung

Die Permanenz und Ubiquität von Daten widerspricht der Funktionsweise der menschlichen Wahrnehmung, welche selektioniert und vergisst. Der Schutz vor Stigmatisierung soll sicherstellen, dass Informationen nur so lange zugänglich sind, wie ein öffentliches Interesse daran besteht. Mit dem Urteil des Europäischen Gerichtshofs (EuGH), wonach nicht an der Quelle gelöscht werden muss, sondern dort, wo die Information auffindbar ist, wird dem Rechnung getragen («Google Spain»-Urteil; «Recht auf Vergessenwerden»).

Auch wenn die Bearbeitung der Daten ursprünglich rechtmässig und sachlich korrekt war, kann sie im Laufe der Zeit unzulässig werden, insbesondere wenn die Daten für ihre ursprüngliche Funktion nicht mehr relevant oder erforderlich sind. In diesem Fall soll die betroffene Person verlangen (können), dass öffentlich zugängliche Ergebnislisten keine Daten mehr anzeigen, die stigmatisierende Informationen über sie enthalten. Dies ermöglicht es den Betroffenen, ihr Leben fortzusetzen, ohne durch die Informationen – länger als zur Wahrung/Umsetzung des öffentlichen Interesses erforderlich – stigmatisiert zu werden.

Entsprechend soll der betroffenen Personen infolge der Löschung der sie benachteiligenden Daten die Möglichkeit zur Entstigmatisierung offen stehen.

4.6 Schutz der offenen Gesellschaft und freien Demokratie

Von Datenbearbeitungen können nicht nur Individuen betroffen sein, sondern auch die Gesellschaft als Ganzes und die freie Demokratie.

Eine offene Gesellschaft ist zum Beispiel durch Social Scoring gefährdet. Social Scoring basiert auf Überwachung und Kontrolle und führt zu Gleichschaltung. Eine funktionsfähige und stabile Demokratie erfordert eine pluralistische, von staatlichem Dirigismus freie Gesellschaft.

Die freie Demokratie ist gefährdet, wenn durch gezielte Informationen oder das bewusste und massenhafte Verbreiten von (Falsch-)Informationen zum Ziel der Manipulation Wahlbeeinflussung stattfindet. Wenn Botschaften zielgerichtet und individuell auf einzelne Personengruppen zugeschnitten werden (und keine Transparenz darüber besteht, wem welche Informationen ausgespielt werden), entsteht die Gefahr, dass der Diskursraum fragmentiert wird. Das kann zu einer Verzerrung der öffentlichen Meinung führen. Der Zugang zu verschiedenen Informationen und Perspektiven muss gewährleistet sein, um eine vielfältige und pluralistische Meinungsbildung im demokratischen Prozess zu ermöglichen.

Abschreckungseffekte («chilling effects»), wonach Menschen aufgrund von Überwachung oder der Angst vor unerwünschten Konsequenzen ihre Grundrechte nicht mehr wahrnehmen, sollen verhindert werden. Ein effektiver Datenschutz schafft die notwendige Vertrauensbasis, um sicherzustellen, dass die Menschen ihre Grundrechte wie Meinungsfreiheit (Art. 16 BV) oder Versammlungsfreiheit (Art. 22 BV) ausüben können, ohne befürchten zu müssen, überwacht und sanktioniert zu werden. Dies ist eine Voraussetzung dafür, dass eine liberale Demokratie bestehen kann.

5 KONZEPT

Basierend auf den Schutzzielen ergibt sich ein Konzept für einen zielgerichteten und wirksamen Datenschutz, der Vertrauen schafft und Innovation fördert. Anstatt die Einwilligung zur Datenbearbeitung und die Zweckbindung in den Mittelpunkt zu stellen, wie es im heutigen Datenschutzdiskurs üblich ist, soll die Wahrung der Schutzziele sowie die Einhaltung und Durchsetzung der substantiellen Mitbestimmung im Zentrum stehen. Das Konzept reguliert den Umgang mit Daten allgemein, anstatt sich ausschliesslich auf Personendaten zu konzentrieren. Zudem werden Grundsätze zur Datenbearbeitung, ein absolutes Verbot für bestimmte Datenbearbeitungen sowie klare Bestimmungen zur Durchsetzung statuiert. So wird ein Rahmen geschaffen, der den Schutz der Rechte der Betroffenen sowie der Gesellschaft als Ganzes gewährleistet.

5.1 Grundsätze

Datenbearbeitungen sind zulässig, sofern ein umfassender Schutz vor widerrechtlichen Datenbearbeitungen besteht. Dieser Schutz wird durch die Wahrung der Schutzziele und der Grundsätze sowie die substantielle Mitbestimmung umfassend gewährleistet. Innerhalb dieses Rahmens sind Datenbearbeitungen erlaubt.

Als Grundsätze gelten:

- Private und staatliche Datenbearbeitungen müssen die Schutzziele für die Individuen und die Gesellschaft wahren.
- Staatliche Datenbearbeitungen brauchen zwingend eine klare gesetzliche Grundlage, aus der eindeutig hervorgeht, welche Daten zu welchem Zweck und wie bearbeitet werden.

5.2 Verbot

Grundsätzlich genügt für die Rechtmässigkeit von Datenbearbeitungen, dass die Einhaltung der Schutzziele sichergestellt ist (und bei staatlicher Datenbearbeitung eine klare gesetzliche Grundlage besteht). Datenbearbeitungen, welche ein grosses Risiko für Individuen oder die Gesellschaft bergen und die Schutzziele nicht gewährleisten können, sind jedoch absolut verboten und können nicht gerechtfertigt werden. Dazu gehören insbesondere biometrische oder anlasslose Massenüberwachung (z.B. Gesichtserkennung im öffentlichen Raum) und Social Scoring.

5.3 Substantielle Mitbestimmung

Das Recht auf informationelle Selbstbestimmung, wie es heute verstanden wird, impliziert, dass jede Person selbst für den Schutz ihrer persönlicher Daten verantwortlich ist. Offensichtlich ist dieses Recht in der Praxis in seiner Wirkungskraft limitiert. Daher stehen die Datenbearbeiter:innen in der Pflicht, die Interessen der Betroffenen zu wahren und die Schutzziele einzuhalten. Unter diesen Gegebenheiten ist eine Datenbearbeitung im Rahmen der Grundsätze unter Einhaltung der Schutzziele ohne Einwilligung möglich.

Zudem sollen die betroffenen Personen durch das Recht auf substantielle Mitbestimmung nicht nur über die (schutzzielkonforme) Bearbeitung ihrer Daten informiert, sondern auch aktiv, unkompliziert und wirksam in den Prozess der Datenbearbeitung eingebunden werden. Kern des Rechts auf substantielle Mitbestimmung ist die Möglichkeit eines einfach wahrnehmbaren Widerspruchsrechts – hinsichtlich der Datenbearbeitung als solche und hinsichtlich der Bearbeitungsmodalitäten wie beispielsweise Anonymisierung. Voraussetzung dafür ist eine umfassende Transparenzpflicht der Datenbearbeiter:innen sowie die Wahrung der gebotenen Sorgfalt. Auf die Rückverfolgbarkeit der Datenbearbeitung, insbesondere bei Weitergabe an Dritte, sowie den Einsatz von automatisierten Entscheidungsfindungssystemen (ADMS), wie künstliche Intelligenz muss deutlich hingewiesen werden.

Dieses Recht auf substantielle Mitbestimmung, führt – gestützt auf den durch die Schutzziele und das Konzept vorgegebenen Rahmen – zu einem deutlich wirksameren und zielorientierteren Datenschutz als das geltende Datenschutzrecht und die informationelle Selbstbestimmung.[2.]

5.4 Datensicherheit

Grundvoraussetzung eines effektiven Datenschutzes ist Datensicherheit. Die Datenbearbeiter:innen haben mit der Pflicht zur Sorgfalt nach anerkannten Regeln der Technik sicherzustellen, dass die Datensicherheit gewährleistet ist und Verletzungen effektiv verhindert werden.

5.5 Durchsetzung

Unter Einhaltung der Schutzziele und unter der Voraussetzung, dass die substantielle Mitbestimmung der Betroffenen sowie die Datensicherheit gewährleistet ist, können Daten und insbesondere auch Personendaten ohne weitere Einschränkungen bearbeitet werden. Ein Missachten der Schutzziele ist unzulässig und stellt einen Verstoss gegen die Regulierung dar. Die Gewährleistung der Schutzziele muss folglich durch wirksame Sanktionen und Mechanismen zur Durchsetzung sichergestellt werden. Insbesondere die Inkaufnahme von grösseren Risiken und eine systematische Verletzung der Grundsätze, Verbote und der substantiellen Mitbestimmung führen zu einer empfindlichen Sanktion.

Gegenüber Wissenschaft, zivilgesellschaftlichen Organisationen, Medien und Behörden soll ein umfassendes Auskunftsrecht bestehen. Verbände und Aufsichtsbehörden sollen das Recht haben, Klage zu erheben. Die zuständige Aufsichtsbehörde sollte verwaltungsrechtliche Sanktionen verhängen können. Bei Erfolg vor Gericht müssen Verbände ihrem Aufwand entsprechend entschädigt werden. Um der Machtasymmetrie zwischen den Datenbearbeiter:innen und den betroffenen Personen entgegenzuwirken, soll eine Beweislastumkehr eingeführt werden. Ausserdem muss die Möglichkeit bestehen, Entscheidungen im Zusammenhang mit dem Einsatz von Automated Decision-Making Systemen (ADMS, künstliche Intelligenz) zu überprüfen, beispielsweise per Datenzugang.

6 AUSWIRKUNGEN

Das Konzept führt unter Einhaltung der Schutzziele zu einem zielgerichteten und wirksamen Datenschutz. Datenbearbeiter:innen werden verstärkt in die Pflicht genommen, die Interessen der betroffenen Personen und der Gesellschaft zu wahren. Individuen haben ein substantielles Mitbestimmungsrecht. Das Vertrauen in die Datennutzung und die Datenbearbeitung wird gestärkt.

1. In der Verfassung (Art. 8 Abs. 2 BV) und im Gesetz (Art. 261bis StGB) wird für die Diskriminierungsdefinition der Begriff «Rasse» verwendet. Das Wort suggeriert ein Menschenbild, das auf der Vorstellung unterschiedlicher menschlicher «Rassen» basiert und steht für eine lange Geschichte rassistischer Gewalt. Damit steht die Verwendung des Begriffs in einem unauflösbaren Widerspruch mit dem Zweck der Bestimmung, wonach eigentlich rassistische Diskriminierung bekämpft werden soll (s.u. https://www.institut-fuer-menschenrechte.de/themen/rassistische-diskriminierung/begriff-rasse; https://www.amnesty.de/glossar-fuer-diskriminierungssensible-sprache).
2. Im DSG ist die Einwilligung der von der Datenbearbeitung betroffenen Person (neben der Rechtfertigung durch ein überwiegendes privates oder öffentliches Interesse oder durch Gesetz) «nur» ein Mittel, wie eine widerrechtliche Persönlichkeitsverletzung geheilt werden kann. Insofern führt diese Möglichkeit der Einwilligung zu einer Schwächung der Betroffenenrechte. Ein einfach wahrnehmbares Widerspruchsrecht – das aus einer Persönlichkeitsverletzung eine widerrechtliche macht – ist nicht vorgesehen, obwohl die Digitale Gesellschaft ein solches bis zum Schluss der Revision des DSG eindringlich gefordert hatte. Die im Datenschutz-Konzept vorgesehene substantielle Mitbestimmung schafft daher in der Praxis mehr informationelle Selbstbestimmung als das bestehende DSG.

Unterstützt durch cms Christoph Merian Stiftung