

Merkblatt Voraussetzungen und Grundsätze für die Bearbeitung von Personendaten (Art. 14 ff. IDAG)

1. Einleitendes

Dieses Merkblatt verschafft den öffentlichen Organen des Kantons Glarus einen Überblick der datenschutzrechtlichen Voraussetzungen und Grundsätze, die es im Umgang mit Personendaten zu beachten gilt. Ob das Datenschutzrecht überhaupt zur Anwendung kommt, hängt davon ab ob Personendaten bearbeitet werden. Werden keine Personendaten bearbeitet, findet das Datenschutzrecht keine Anwendung.

2. Wann liegen überhaupt Personendaten vor?

2.1. Personendaten

Personendaten sind Informationen, die sich auf eine bestimmte oder bestimmbare *natürliche* Person beziehen. Die Grenze der Bestimmbarkeit ist weit zu ziehen. Informationen sind nicht nur dann einer Person zuordenbar, wenn eine direkte Identifikation möglich ist, sondern auch dann, wenn die Identifikation mit verhältnismässigem Abklärungsaufwand möglich ist oder durch Kombination verschiedener Informationen indirekt gelingt.

2.2. Besonders schützenswerte Personendaten

Bei der Bearbeitung von besonders schützenswerten Personendaten besteht eine erhöhte Gefahr für Persönlichkeits- oder Grundrechtsverletzungen von Betroffenen. In solchen Fällen müssen die datenschutzrechtlichen Vorschriften besondere Beachtung finden. Je nach Kontext oder in Kombination können auch gewöhnliche Personendaten als besonders schützenswert eingestuft werden. Eine abschliessende Nennung aller besonders schützenswerter Personendaten ist jedenfalls nicht möglich. Besonders schützenswert sind in etwa Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten, Daten über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse oder Ethnie, genetische Daten und biometrische Daten, die eine natürliche Person eindeutig identifizieren, aber auch Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen sowie Daten über Massnahmen der sozialen Hilfe oder fürsorgerische Massnahmen (Art. 6 Abs. 1 VIDAG).

2.3. Stammdaten

Stammdaten sind ebenfalls Personendaten. Bei deren Bearbeitung besteht jedoch eine geringe Gefahr für eine Persönlichkeits- oder Grundrechtsverletzung. Als Stammdaten gelten abschliessend Name, Vorname, Adresse, Geburtstag, Heimatort (Art. 7 Abs. 1 VIDAG).

Zusammengefasst kann gesagt werden, dass sofern öffentliche Organe Stammdaten, Personendaten und/oder besonders schützenswerte Personendaten von natürlichen Personen bearbeiten, so haben sie die datenschutzrechtlichen Vorschriften einzuhalten (Art. 1 Abs. 1 Bst. c. i.V.m. Art. 5 IDAG), worunter auch die Voraussetzungen und Grundsätze für die Bearbeitung von Personendaten fallen.

3. Voraussetzungen für die Bearbeitung von Personendaten

Das Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (IDAG) bestimmt die Voraussetzungen, die erfüllt sein müssen, damit Personendaten bearbeitet werden dürfen.

3.1. Rechtmässigkeit (Art. 14 IDAG)

Öffentliche Organe dürfen Personendaten nur bearbeiten, wenn dies rechtmässig erfolgt. Wenn es an der Rechtmässigkeit der Datenbearbeitung fehlt, dann handelt es sich grundsätzlich um eine Persönlichkeitsverletzung der Betroffenen.

Ob eine Bearbeitung rechtmässig ist, gilt es nach den gesetzlichen Voraussetzungen gemäss Art. 14 Abs. 1 – bzw. Abs. 2 IDAG im Umgang mit besonders schützenswerten Personendaten – zu bestimmen: Im Regelfall bedarf es zur rechtmässigen Bearbeitung von Personendaten einer gesetzlichen Grundlage oder einer gesetzlichen Aufgabe, die zur Bearbeitung ermächtigt (Art. 14 Abs. 1 Bst. a. und b. IDAG). Werden besonders schützenswerte Personendaten bearbeitet, bedarf es einer Grundlage im Gesetz selbst oder aber die Bearbeitung muss zur Erfüllung einer im Gesetz klar umschriebenen Aufgabe erforderlich sein (Art. 14 Abs. 2 Bst. a. und b. IDAG). Im Einzelfall kann anstelle auf die gesetzliche Grundlage auch auf eine Einwilligung (Art. 14 Abs. 1 Bst. c. IDAG sowie Art. 14 Abs. 2 Bst. c. IDAG) oder aber auf eine stillschweigende Einwilligung der betroffenen Person abgestellt werden (Art. 14 Abs. 1 Bst. d. und f. IDAG sowie Art. 14 Abs. 2 Bst. d. und f. IDAG). Eine Einwilligung ist dann rechtsgenügend, wenn sie nach angemessener Information – sprich in Kenntnis der Sachlage –, freiwillig und eindeutig beziehungsweise für die Bearbeitung besonders schützenswerter Daten und das Profiling ausdrücklich erteilt worden ist. Sie ist auf den Einzelfall beschränkt und kann jederzeit widerrufen werden (Art. 14 Abs. 3 IDAG). Erfolgt die Beschaffung auf Grundlage einer mutmasslichen Einwilligung im Sinne von Art. 14 Abs. 1 Bst. e. bzw. Art. 14 Abs. 2 Bst. e. IDAG, so sind die Voraussetzungen der mutmasslichen Einwilligung zu beachten.

Eine Einwilligung in die Bekanntgabe von Gesundheitsdaten an eine ärztliche Fachperson ist auf den Einzelfall zu beschränken. Zudem kann sie erst nach angemessener Information freiwillig und ausdrücklich erfolgen. Unzulässig wäre es etwa, beim Eintritt in ein Altersheim eine zeitlich unbeschränkte Einwilligung in die Bekanntgabe von Gesundheitsdaten über den gesamten Aufenthaltszeitraum bzw. über alle künftigen Behandlungen zu verlangen.

3.2. Verhältnismässigkeit (Art. 15 IDAG)

Öffentliche Organe dürfen nur diejenigen Personendaten bearbeiten, die für die Erfüllung ihrer öffentlichen Aufgabe in persönlicher, sachlicher und zeitlicher Hinsicht geeignet und erforderlich sind (Art. 15 Abs. 1 IDAG). Ob eine Bearbeitung von Personendaten verhältnismässig ist, kann sich jeweils nur aus dem konkreten Einzelfall ergeben.

Die Datenbearbeitung muss geeignet sein, um den mit der Bearbeitung verfolgten Zweck bzw. die Erfüllung der gesetzlichen Aufgabe erfüllen zu können. Je präziser eine Datenbearbeitung auf die Erfüllung der gesetzlichen Aufgabe zugeschnitten ist, desto eher erscheint die Bearbeitung als geeignet.

Ungeeignet ist eine Datenbearbeitung etwa dann, wenn der Datenbestand, der genutzt wird, um automatisierte Einzelentscheide (bspw. Verfügungen) zu fällen, nicht oder nur teilweise aktuell geführt würde. Da die zugrundeliegenden Informationen bereits unrichtig sind, wären auch die (einzelne) Entscheide fehlerhaft und somit von Grund auf ungeeignet.

Erforderlich ist die Datenbearbeitung regelmässig nur dann, wenn keine mildereren Mittel nebst der Datenbearbeitung vorliegen, die gleich geeignet sind zur Zweck- bzw. gesetzlichen Aufgabenerfüllung. Sodann muss eine persönliche, zeitliche, sachliche und räumliche Erforderlichkeit vorliegen, damit die Bearbeitung als verhältnismässig erachtet werden kann.

Mit **Erforderlichkeit in persönlicher Hinsicht** ist etwa gemeint, dass die Anzahl von Personen, die von der Datenbearbeitung betroffen sind, auf das tatsächlich erforderliche Mindestmass reduziert wird. An einer **sachlichen Erforderlichkeit** fehlt es bspw. dann, wenn Personendaten ohne eigentlichen Bearbeitungszweck erhoben und gespeichert werden, also eine Datenerhebung auf Vorrat erfolgt. Auch muss die **Erforderlichkeit in zeitlicher Hinsicht** gegeben sein, so dass etwa Personendaten nur solange gespeichert werden, wie es der Bearbeitungszweck erfordert. Ist der Bearbeitungszweck erfüllt, müssen die Personendaten grundsätzlich umgehend vernichtet werden. Im Zusammenhang mit der Videoüberwachung von öffentlichem Grund spielt sodann die **räumliche Erforderlichkeit** eine entscheidende Rolle. Demnach dürften nur jene Bereiche des öffentlichen Raums durch Videoanlagen überwacht werden, die zur Erfüllung des Überwachungszwecks tatsächlich erforderlich sind.

Die Bearbeitung von Personendaten muss sodann zumutbar sein, sprich die mit der Bearbeitung verfolgten Zwecke, welche immer im öffentlichen Interesse liegen müssen, dürfen in keinem Missverhältnis zu den tangierten Persönlichkeits- und Grundrechte der betroffenen Personen stehen.

Ein solches Missverhältnis liegt etwa dann vor, wenn anlasslos Personendaten von Bürgerinnen und Bürgern erhoben, gespeichert und weiterbearbeitet werden, um einer diffusen, nicht näher konkretisierten Gefahrenlage der öffentlichen Sicherheit und Ordnung begegnen zu wollen oder aber um einem einseitig gelagerten Sicherheitsbedürfnis gerecht werden zu wollen.

4. Grundsätze für die Bearbeitung von Personendaten

Die Grundsätze nach denen Personendaten durch öffentliche Organe bearbeitet werden dürfen, sind im Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (IDAG) geregelt. Der Grundsatz von Treu und Glauben ist im Datenschutzrecht nicht explizit statuiert, gilt aber als Verfassungsgrundsatz auch ungeschrieben.

4.1. Richtigkeit (Art. 16 IDAG)

Personendaten müssen richtig und, soweit es der Zweck des Bearbeitens verlangt, vollständig und aktuell sein (Art. 16 Abs. 1 IDAG). Personendaten sind dann richtig, wenn sie eine Tatsache oder einen Umstand im Hinblick auf den Bearbeitungszweck sachgerecht wiedergeben. Unrichtig sind Personendaten etwa dann, wenn sie – in Abhängigkeit des jeweiligen Sachzusammenhangs – unvollständig oder nicht aktuell geführt sind. Als Korrelat des Grundsatzes der Datenrichtigkeit gilt das Berichtigungsrecht der Betroffenen gemäss Art. 39 IDAG, worauf gestützt Betroffene vom verantwortlichen öffentlichen Organ verlangen können, unrichtige Personendaten berichtigten zu lassen. Die Beweislast für die Richtigkeit trägt das öffentliche Organ. Die betroffene Person hat jedoch bei der Abklärung mitzuwirken (Art. 16 Abs. 2 IDAG). Die Mitwirkung erfolgt bspw. durch die Erteilung von Auskünften oder die Vorlage von erforderlichen Dokumenten. Der Umfang der Mitwirkungspflicht muss jedoch verhältnismässig sein, womit etwa gemeint sein kann, dass die Mitwirkung der Betroffenen zur Abklärung der Richtigkeit erfüllbar und zumutbar sein muss.

Im Rahmen des (kantonalen) Bedrohungsmanagements werden Persönlichkeitsaspekte einer Person unrichtig erhoben oder aber ein Informatikmittel, das die Legalprognose der betroffenen Person bewerten soll, liefert unrichtige Ergebnisse. Als mögliche Konsequenz wird besagte Person als Gefährder eingestuft und mit präventiv-polizeilichen Massnahmen belegt.

4.2. Datensicherheit (Art. 17 IDAG; Art. 8 – 13 VIDAG)

Personendaten müssen durch angemessene organisatorische und technische Massnahmen gesichert werden (zum Katalog möglicher Massnahmen siehe Art. 12 und 13 VIDAG), sodass eine Verletzung der Datensicherheit vermieden werden kann (Art. 17 Abs. 1 IDAG). Verletzungen der Datensicherheit können bspw. zu materiellen und/oder immateriellen Schädigungen von Betroffene führen. Denkbar ist etwa, dass eine Medikationsliste unrichtig geführt wird und Patientinnen und Patienten deswegen nicht oder nur teilweise die verschriebene Medikation erhalten (dazu unten 4.2.3 Integrität). Der Grundsatz der Datensicherheit richtet sich an den nachfolgend beschriebenen Schutzziele der Vertraulichkeit, der Verfügbarkeit, der Integrität und der Nachvollziehbarkeit von Personendaten

4.2.1. Vertraulichkeit

Gemeint ist, dass Informationen nur Berechtigten zugänglich sein dürfen. Der Kreis der Berechtigten ergibt sich aus dem Kontext der jeweiligen gesetzlichen Aufgabenerfüllung sowie dem Inhalt und der Bedeutung der Information, wobei die Gewährung von Zugriffsberechtigungen verhältnismässig erfolgen muss. Entsprechend kann der Kreis der Berechtigten auf wenige Personen beschränkt oder aber auch grösser sein.

Informationen zum Aufenthalt und zum Gesundheitszustand (bspw. zu Diagnostik und Therapie) von Menschen in psychiatrischen Kliniken, gelten aus verschiedenen Gründen als besonders schützenswerte Personendaten, weshalb sie einer strikten Vertraulichkeit unterstehen. Zu deren Schutz bedarf es umfassender organisatorischer und technischer Massnahmen (zu möglichen Massnahmen siehe Art. 12 und 13 VIDAG), damit die Informationen nicht Unberechtigten zugänglich gemacht werden.

4.2.2. Verfügbarkeit

Für die Entscheidungs- und Handlungsfähigkeit öffentlicher Organe ist es erforderlich, dass sie im Rahmen der gesetzlichen Aufgabenerfüllung die notwendigen Informationen rechtzeitig, in gewünschter Form und am gewünschten Ort abrufen können. Die Anforderungen an die Verfügbarkeit von Informationen sind höher, wenn diese für die Erfüllung von wesentlichen Aufgaben unterbruchlos vorhanden sein müssen.

Das Informatikmittel, mit welchem die ordnungsgemässe und fristgerechte Entlohnung des Staatspersonals sichergestellt werden soll, fällt aus. Aufgrund des Totalausfalls werden die Löhne kurz vor Weihnachten verspätet ausbezahlt.

4.2.3. Integrität

Die Datenintegrität steht im engen Verhältnis zum Grundsatz der Richtigkeit (siehe auch Ausführungen oben 4.1. Richtigkeit). Die Wahrung der Unversehrtheit und Richtigkeit bedingt jedoch, dass durch Bearbeitungsvorgänge keine unzulässigen Änderungen an den Daten vorgenommen werden können.

Eine in einer Gesundheitsinstitution geführte Medikationsliste wird durch eine nicht bearbeitungsberechtigte Person verfälscht (Liste wurde nicht vor unberechtigten Zugriffen geschützt). In der Folge erhalten gewisse Patientinnen und Patienten nicht oder nur teilweise die verschriebene Medikation. Aufgrund der falschen Medikation nimmt ein Patient körperlichen Schaden, da ihm eine zu hohe Dosis verabreicht wurde.

4.2.4. Nachvollziehbarkeit

Die nachvollziehbare Bearbeitung der Informationen ist bspw. für alle öffentlichen Verfahren (Strafverfahren, Beschwerdeverfahren usw.) von grosser Bedeutung, aber auch für die Erfüllung von Kontroll- und Aufsichtsaufgaben sowie für das Vorgehen bei Missbräuchen.

Ein Staatsangestellter, dem Zugriff auf die kantonale Datenplattform (GERES) gewährt wurde, nutzt seine Zugriffsrechte, um Informationen über seine Nachbarschaft in Erfahrung zu bringen. Da die Einsichtnahme nicht in Erfüllung einer gesetzlichen Aufgabe erfolgt, handelt es sich um eine missbräuchliche Datenbearbeitung. Um den Missbrauch nachvollziehen zu können, müssen die einzelnen Zugriffe protokolliert (Art. 13 VIDAG) und somit nachvollziehbar gemacht werden.

4.3. Zweckbindung (Art. 18 IDAG)

Personendaten dürfen nur zu dem Zweck bearbeitet werden, welcher bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist. Der Grundsatz der Zweckbindung soll es der von einer Datenbearbeitung betroffenen Person ermöglichen, dass sie bereits zu Beginn weiss, wofür ihre Daten verwendet werden und dass die Daten nicht zweckentfremdet werden. Dadurch, dass ersichtlich wird zu welchem Zweck Personendaten bearbeitet werden, wird auch Transparenz für die betroffenen Personen geschaffen. Zweckbindung meint aber auch, dass Daten nicht ohne nähere Zweckbestimmung auf Vorrat erhoben oder nach der Zweckerfüllung weiter aufbewahrt werden dürfen. Ein Abweichen vom Zweckbindungsgebot ist nur zulässig, sofern dafür die Voraussetzungen für das Bearbeiten von Personendaten (siehe oben Rechtmässigkeit (Art. 15 IDAG) und Verhältnismässigkeit (Art. 16 IDAG)) erfüllt sind, wobei die Grundsätze der Personendatenbearbeitung ebenfalls zu beachten sind.

- Die von den Einwohnerkontrollen geführten Daten zum Wohnsitz und zur Ausländerkategorie von Bürgerinnen und Bürger dürfen nicht mittels automatisiertem Export aus der kantonalen Datenplattform (GERES) bezogen werden, um eine allfällige Beitragsberechtigung von pflegenden und betreuenden Bezugspersonen ermitteln zu können. Als die betroffenen Personen den Einwohnerkontrollen in der Vergangenheit entsprechende Personendaten bekanntgaben, war für sie nicht ersichtlich, dass der meldepflichtige Wohnsitz und die Ausländerkategorie je einmal für die Ermittlung der Beitragsberechtigung genutzt würden. Eine Bekanntgabe und Weiterbearbeitung dieser Daten käme einer Zweckentfremdung gleich. Um die Daten nutzen zu dürfen, müsste vorgängig eine entsprechende gesetzliche Grundlage inkl. neuem Bearbeitungszweck geschaffen werden.
- Eine Datenerhebung auf Vorrat, ohne dass die Erhebung der Erfüllung einer gesetzlichen Aufgabe dient, würde zweckgebunden erfolgen und wäre demnach unzulässig.

4.4. Datenvermeidung und Datensparsamkeit (Art. 19 IDAG)

Die Grundsätze der Datenvermeidung und Datensparsamkeit stehen insofern in engem Zusammenhang zum Verhältnismässigkeitsgrundsatz, als dass öffentliche Organe angehalten sind, mengenmässig nur das tatsächlich Erforderliche an Personendaten zu erheben. Wenn immer möglich, sollen keine oder möglichst wenig Personendaten erhoben, weiterbearbeitet und gespeichert werden, was auch bedingt, dass die Bearbeitung von Personendaten auf das für den Verwendungszweck nötige Mindestmass beschränkt ist und gespeicherte Daten regelmässig vernichtet werden sobald der Verwendungszweck nicht mehr gegeben ist. Mittels Anonymisierung und Pseudonymisierung (Art. 9 IDAG) von Personendaten besteht sodann eine Möglichkeit, den Personenbezug (vorübergehend) aus einer Gesamtinformation zu entfernen, womit den Grundsätzen der Datenvermeidung und Datensparsamkeit ebenfalls Rechnung getragen werden kann.

5. Weitere Grundsätze für die Bearbeitung von Personendaten

5.1. Grundsatz von Treu und Glauben

Die Bearbeitung von Personendaten hat nach Treu und Glauben zu erfolgen (vgl. Art. 5 Abs. 3 Bundesverfassung und Art. 17 Abs. 1 Verfassung Kanton Glarus). Gemeint ist, dass die öffentlichen Organe ein loyales und vertrauenswürdiges Verhalten im Umgang mit Personendaten an den Tag legen.

Im Zuge der Datenbeschaffung informiert das öffentliche Organ die betroffenen Personen darüber, welche Personendaten erhoben werden, zu welchem Zweck die Daten bearbeitet und an wen diese bekanntgegeben werden (vgl. Art. 21 Abs. 1 IDAG). Gibt das öffentliche Organ an, dass die Daten nicht an Dritte bekannt gegeben werden, so ist es durch den Grundsatz von Treu und Glauben an diese Auskunft gebunden und darf die Daten demnach nicht weitergeben.

5.2. Grundsatz der Transparenz (insb. Art. 21 IDAG)

Der Grundsatz der Transparenz ist insbesondere im Zusammenhang mit der Beschaffung von Personendaten von Relevanz. Zum Grundsatz der Transparenz und den Informationspflichten gemäss Art. 21 IDAG wird auf das Merkblatt «Informationspflichten gem. Art. 21 IDAG sowie Art. 14 und 15 VIDAG» verwiesen.