Information zur Datenschutzgrundsatzverordnung

Spätestens nach der „Newsletter-Opting-In-Opting-Out"-Flut, mit der wir alle konfrontiert waren, muss klar gewesen sein: Es tut sich etwas im Datenschutz und das Wort des Jahres wird am Ende „Einwilligung" sein.

Seit 25.05.2018 gilt die Datenschutzgrundverordnung (DSGVO) und schafft einen neuen Rechtsrahmen im Bereich des Datenschutzes. Die Gemeinde hat diese bereits umgesetzt und wird nun bis Ende des Jahres eine Vertiefung stattfinden.

Zum Hintergrund

Die DSGVO wird vielfach als neuer Meilenstein im Datenschutzbereich beschrieben. Ohne Zweifel bedeutet sie die größte Änderung im Datenschutzrecht seit mehr als 20 Jahren. Die DSGVO löst die bisherige Datenschutz-Richtlinie aus dem Jahre 1995 ab. Neue technologische Entwicklungen haben den Datenschutz seither vor große Herausforderungen gestellt. Die Themen Cloud, Big Data, Social Media, Internet der Dinge, Industrie 4.0 waren 1995 noch weitgehend unbekannt. Diese technologischen Entwicklungen haben dazu geführt, dass generell immer mehr und mehr Daten weltweit verarbeitet werden.

Dazu kommt, dass der private Umgang gerade mit Social Media (Facebook, Whatsapp, etc) erschreckend naiv und unkritisch ist.

Im 1. Quartal 2018 wurden allein bei Facebook rund 2,2 Milliarden Monthly Active Users (MAUs) gezählt. In Deutschland wird Facebook von rund 30 Millionen Personen genutzt (Stand: Mai 2017). Nach einem Ranking der Social Networks in Deutschland mit dem größten Marktanteil - gemessen an dem Anteil der Unique User - belegte Facebook mit rund 35 Prozent den ersten Platz. Der Umsatz des Social Media-Unternehmens belief sich im Jahr 2017 auf rund **40,65 Milliarden US-Dollar**. Mit rund 39,94 Milliarden US-Dollar wurde der größte Umsatzanteil im Segment Werbung erzielt. Im gleichen Jahr konnte das Unternehmen einen Gewinn in Höhe von rund 15,93 Milliarden US-Dollar ausweisen (Quelle: © Statista 2018).

Wie die aktuellen Medienberichte über Facebook und Cambridge Analytica zeigen, besteht durchaus die Gefahr, dass Daten missbräuchlich verwendet werden.

Die DSGVO hat sich das ambitionierte Ziel gesetzt, die Rechte der Bürger zu stärken und ihnen die Kontrolle über ihre persönlichen Daten zurückzugeben. Hier zur Ihrer ersten Selbstkontrolle unsere Standardfragen:

- Können Sie nachweisen, ob Sie zu dem einen oder anderen Newsletter überhaupt Ihre Zustimmung erteilt haben?
- Haben Sie jemals die Datenschutzerklärung zu einem Online-Shop bis zum Ende durchgelesen?
- Können Sie erklären, was Cookies sind? –Schließlich stimmen Sie diesen täglich zu, bevor Sie Ihre Tageszeitung überhaupt zu lesen beginnen (können)?
- Haben Sie sich schon einmal gefragt, ob Ihr Arbeitgeber protokolliert, welche Internetseiten Sie (in der Pause natürlich) am Arbeitsplatz aufrufen?
- Haben Sie einen Überblick über Ihre tatsächlichen Datenspeicherorte? (zu Hause, innerhalb der EU, in einem Drittland wie Indien oder Südafrika?)
- Haben Sie sich schon einmal aktiv gefragt, ob Ihr Kind in zwanzig Jahren mit Kinderfotos "auf Facebook" überhaupt sein will? Wollen Sie Ihr Kind nicht zu einem späteren Zeitpunkt selbst entscheiden lassen, welche Daten es von sich aus freiwillig preisgeben möchte?

Behörden, Unternehmen und Organisationen trifft im Ergebnis nun künftig jedenfalls eine erhöhte **Selbstverantwortung** bei der Verarbeitung von personenbezogenen Daten. Es gelten erweiterte Dokumentationspflichten sowie strengere Vorgaben für Datensicherheit. Einer der Kernpunkte der Reform sind zudem die strengen Sanktionen, die dem Datenschutz mehr Beachtung schenken sollen.

Drei Wochen vor Inkrafttreten der DSGVO hat die österreichische Regierung jedoch noch viele Aufweichungen mit dem sogenannten Datenschutz-Anpassungsgesetz 2018, das neben der DSGVO zu beachten ist, vorgenommen. Beispielsweise werden viele Strafen nun erst bei wiederholtem Verstoß schlagend. Die Datenschutzbehörde soll im Sinne der "Verhältnismäßigkeit" im Erstfall einer Datenschutzverletzung nur eine Verwarnung aussprechen. Behörden (zB Bürgermeister, Bezirkshauptmann, Landeshauptmann) können für viele Verstöße faktisch nicht mehr belangt werden.

Es bleibt auch wie bisher schwer, gegen große Konzerne wie Facebook vorzugehen, zumal diese in der Regel keinen Sitz in Österreich haben.

Erleichtert wird allerdings die Videoüberwachung, die nun auch eingesetzt werden darf, wenn es theoretisch "gelindere Mittel" gäbe, um eine Person oder ein Objekt zu schützen. Zudem dürfen Fotos und Videos nun mit anderen personenbezogenen Daten abgeglichen werden. Eine Zustimmung des oder der Betroffenen ist nicht erforderlich. Explizit verboten ist ohne Einwilligung nur die Erstellung von "Persönlichkeitsprofilen", die allerdings nicht genau definiert werden.

Die im Gesetzestext verankerte Aufforderung an die Datenschutzbehörde, hauptsächlich Verwarnungen auszusprechen, wird bereits zurecht als "europarechtswidrig" kritisiert und stehen in den nächsten Jahren – zumindest für alle Datenschützer – spannende Zeiten an.

Die bestehende Meldepflicht bei Datenschutzverletzungen wird mit der DSGVO wesentlich ausgeweitet. Künftig muss bei jedem Datenleck die Aufsichtsbehörde binnen 72 Stunden ab Kenntnis im Detail informiert werden, soweit nicht jegliches Risiko für die Rechte und Freiheiten betroffener Personen ausgeschlossen werden kann. Im Fall eines hohen Risikos für die betroffenen Personen müssen diese persönlich informiert werden.

Die Verantwortlichen müssen künftig ein schriftliches Verzeichnis der Verarbeitungstätigkeiten führen. Dafür entfällt die bisherige Meldepflicht gegenüber dem Datenverarbeitungsregister. Für Datenverarbeitungen, bei denen das Risiko einer Verletzung von Rechten betroffener Personen voraussichtlich besonders hoch ist, ist vom Verantwortlichen vor Beginn der Datenverarbeitung eine Datenschutz-Folgenabschätzung durchzuführen. Dies betrifft insb Verarbeitungen, die der systematischen und umfassenden Bewertung persönlicher Aspekte natürlicher Personen dienen und/oder bei denen öffentlich zugängliche Bereiche systematisch umfangreich überwacht werden.

Schließlich müssen Behörden und Unternehmen, zu deren Kerntätigkeit die umfangreiche Verarbeitung sensibler Daten oder die umfangreiche und systematische Überwachung natürlicher Personen gehört, künftig einen Datenschutzbeauftragten bestellen.

Für wen gilt die DSGVO?

Die DSGVO gilt für die Verarbeitung **personenbezogener Daten**, dh jeglicher Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Bei der Frage, ob es sich um eine identifizierbare Person handelt, ist nicht nur auf das Wissen und die rechtlichen und tatsächlichen Möglichkeiten des jeweiligen Verantwortlichen abzustellen, der die Daten konkret verarbeitet. Für den Personenbezug genügt bereits die Identifikationsmöglichkeit durch einen Dritten.

Eine IP-Adresse eines Nutzers ist daher für einen Websitebetreiber auch dann personenbezogen, wenn nur der Internet Access Provider den Nutzer anhand der IP-Adresse identifizieren kann.

Anonyme Daten, die von niemandem auf eine bestimmte Person rückgeführt werden können, sind datenschutzrechtlich nicht relevant. Nach der DSGVO künftig nicht mehr geschützt, sind Daten über juristische Personen.

Explizit ausgenommen von der DSGVO ist die Verarbeitung personenbezogener Daten durch natürliche Personen zu ausschließlich **persönlichen oder familiären Zwecken.** Für rein private Aktivitäten in sozialen Medien gilt die DSGVO daher nicht.

Sie müssen also zumindest keine Betroffenenrechte nach der DSGVO beantworten, wenn Sie in Ihrem Smartphone die privaten Kontaktdaten Ihrer Freundin speichern.

Wo gilt die DSGVO?

Die DSGVO gilt in jedem Fall für Verantwortliche und Auftragsverarbeiter, die ihren Sitz innerhalb der EU haben sowie für die Verarbeitung im Rahmen der Tätigkeiten einer (selbständigen oder unselbständigen) Niederlassung in der EU.

Eine wesentliche Neuerung ist die Erweiterung des Anwendungsbereichs auf nicht in der EU niedergelassene Verantwortliche und Auftragsverarbeiter, wenn diese Daten von betroffenen Personen, die sich in der EU aufhalten, verarbeiten, um ihnen Waren oder Dienstleistungen anzubieten oder um ihr Verhalten zu beobachten (Profiling). Letzteres betrifft insb die Beobachtung Ihres Surfverhaltens, um gezielt Werbung zu betreiben.

Datenschutzrechtliche Grundsätze

Bei jeder Verarbeitung personenbezogener Daten müssen die allgemeinen datenschutzrechtlichen Grundsätze eingehalten werden.

Wie bisher gelten der **Grundsatz der Rechtmäßigkeit** und der Verarbeitung nach **Treu und Glauben**. Dabei geht es um eine faire Verarbeitung. Wesentlich ist die ausreichende Information der betroffenen Personen. Diese dürfen über die Umstände der Verarbeitung und ihre Rechte nicht in die Irre geführt oder im Unklaren gelassen werden. Dies ergibt sich auch aus dem **Transparenzgrundsatz.** Daten müssen in einer für die betroffenen Personen nachvollziehbaren Weise verarbeitet werden. Die Transparenz ist für die betroffenen Personen Voraussetzung für die Kontrolle über die Verwendung der eigenen Daten und damit wesentlich für den Datenschutz. Der Transparenzgrundsatz wird durch **umfangreiche Informationspflichten**, die bei jeder Erhebung von Daten zu beachten sind, konkretisiert.

Eine zentrale Rolle im Datenschutzrecht spielt der **Zweckbindungsgrundsatz.** Daten dürfen nur für **festgelegte, eindeutige und rechtmäßige Zwecke** ermittelt und weiterverwendet werden.

Ausgangspunkt für die Prüfung der Zulässigkeit der Datenverarbeitung ist stets der jeweilige Verarbeitungszweck. Sollen Daten später für einen anderen Zweck weiterverwendet werden, ist zu prüfen, ob hierfür eine ausreichende Rechtsgrundlage besteht. Neu ist, dass Daten ausnahmsweise auch für einen anderen Zweck weiterverwendet werden dürfen als jenen, für den die Daten ursprünglich erhoben wurden, sofern der ursprüngliche und der neue Zweck miteinander vereinbar sind. Die

Vereinbarkeit ist stets anhand einer Reihe von Kriterien zu prüfen, ua ausgehend von den vernünftigen Erwartungen der betroffenen Personen.

Nach dem **Grundsatz der Datenminimierung** dürfen Daten nur verwendet werden, soweit sie für den jeweiligen Verarbeitungszweck wesentlich sind und über das erforderliche Ausmaß nicht hinausgehen. Mit Daten ist daher möglichst sparsam umzugehen.

Nach dem **Grundsatz der Speicherbegrenzung** dürfen Daten darüber hinaus nur so lange in personenbezogener Form aufbewahrt werden, als dies für die Erreichung der Zwecke, für die sie ermittelt wurden, erforderlich ist. Danach sind die Daten zu löschen oder zu anonymisieren, soweit die Daten nicht aufgrund gesetzlicher Verpflichtungen länger aufbewahrt werden müssen.

Nach dem **Grundsatz der sachlichen Richtigkeit und Aktualität** dürfen Daten nur so verwendet werden, dass sie im Hinblick auf den Verwendungszweck sachlich richtig sind. Wenn nötig, sind sie zu aktualisieren.

Der **Grundsatz der Datenintegrität und Vertraulichkeit** erfordert, dass angemessene technische und organisatorische Datensicherheitsmaßnahmen getroffen werden.

Die DSGVO statuiert nun ausdrücklich eine **Rechenschaftspflicht** des Verantwortlichen. Dieser muss die Einhaltung der obigen Grundsätze nachweisen können und daher entsprechend dokumentieren. Nach Möglichkeit sind die Grundsätze durch geeignete technische und organisatorische Maßnahmen umzusetzen.

Rechtmäßigkeit der Verarbeitung

Die DSGVO verfolgt - wie auch schon bisher das DSG 2000 - das Prinzip, dass jede Verarbeitung personenbezogener Daten verboten ist, soweit diese nicht unter einen **Erlaubnistatbestand** fällt.

Eine Verarbeitung "normaler" (z.B. Vorname, Nachname, Adresse, Geburtsdatum), nicht sensibler Daten (z.B. Gesundheitsdaten) ist nur rechtmäßig, wenn die betroffene Person ihre **Einwilligung** erteilt hat, die Daten zur **Erfüllung** eines Vertrags mit der betroffenen Person verarbeitet werden, eine **gesetzliche Verpflichtung** besteht, die Verarbeitung dem **Schutz lebenswichtiger Interessen** oder der **Erfüllung öffentlicher Aufgaben** dient, oder der Verantwortliche ein **berechtigtes Interesse** an der Verarbeitung hat, soweit die Interessen der betroffenen Person nicht überwiegen. Sensible Daten dürfen nur unter noch strengeren Voraussetzungen verarbeitet werden.

Wie bisher muss eine Einwilligung **in informierter Weise**, in Kenntnis der Sachlage erfolgen. Schriftliche Ersuchen um Einwilligung müssen in verständlicher Form, in klarer und einfacher Sprache erfolgen. Neu ist, dass eine Einwilligung stets **aktiv** erteilt werden muss. Eine bereits angehakte Checkbox reicht daher nicht.

Besondere Anforderungen gelten künftig hinsichtlich der **Freiwilligkeit** einer Einwilligung. Eine Einwilligung ist nur dann freiwillig, wenn die betroffene Person die Einwilligung verweigern kann, ohne daraus Nachteile zu erleiden.

Einwilligungen zu verschiedenen Verarbeitungszwecken müssen gesondert erteilt werden können. Die Erfüllung eines Vertrags einschließlich der Erbringung einer Dienstleistung darf nicht von einer Einwilligung abhängig gemacht werden, die für die Erfüllung des Vertrags nicht erforderlich ist.

In der Praxis kommt es vor allem im Internet häufig vor, dass bestimmte Services nur dann genutzt werden können, wenn die Nutzer einer Nutzung ihrer Daten für Werbezwecke zustimmen. Nach der DSGVO sind derartige Geschäftsmodelle nur eingeschränkt zulässig. Die DSGVO sieht kein absolutes **Koppelungsverbot** vor.

Denkbar wäre etwa, den Nutzern eine Wahlmöglichkeit zu bieten zwischen einem kostenlosen werbefinanzierten Modell, bei dem die Nutzer mit ihren Daten bezahlen, und einem kostenpflichtigen werbefreien Modell. Hier warten wir gespannt, wie digitale Medien dies umsetzen werden.

Bei der Einholung einer Einwilligung muss auf das jederzeitige **Widerrufsrecht** hingewiesen werden. Bestehende Einwilligungen, die nicht den Anforderungen der DSGVO entsprechen, sind nicht verbindlich und müssen daher ggf neu eingeholt werden.

Rechte der betroffenen Person

1. Modalitäten für die Ausübung der Betroffenenrechte

Eine weitere Konsequenz der DSGVO ist, dass Sie nun auf Ihre Betroffenenrechte (zB auf der Website) hingewiesen werden:

Art 12 enthält allgemeine Bestimmungen, die für alle Betroffenenrechte gem Art 13 bis 22 DSGVO relevant sind. Der Verantwortliche ist verpflichtet, der betroffenen Person alle Informationen bzw Mitteilungen "in **präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache**" zu übermitteln. Ferner muss der Verantwortliche der betroffenen Person die Ausübung ihrer Rechte möglichst erleichtern und eine Antragstellung auf elektronischem Wege ermöglichen, also per E-Mail.

Davon gibt es eine Ausnahme für offenkundig unbegründete oder - insb im Fall von häufiger Wiederholung - exzessive Anträge. Diesfalls kann der Verantwortliche ein angemessenes Entgelt fordern, das die Verwaltungskosten der Informationserteilung oder die Durchführung der Maßnahme abdeckt, oder den Antrag überhaupt ablehnen.

2. Aktive Informationspflichten

Bei jeder Erhebung von personenbezogenen Daten sind die aktiven Informationspflichten zu beachten. Die DSGVO sieht eine Reihe von Pflichtangaben bei der Erhebung von Daten bei den betroffenen Personen vor.

Dies gilt insb für diverse Web- und Papierformulare, die von den betroffenen Personen auszufüllen sind (zB Anmelde- und Registrierungsformulare, Fragebögen, Anträge etc), auch wenn die Erhebung der Daten gesetzlich vorgesehen ist oder wenn die Daten zur Vertragserfüllung benötigt werden. Im Vergleich zur bisherigen Rechtslage wurden die Informationspflichten wesentlich ausgeweitet. So sind nun neben der Identität des für die Verantwortlichen und dem Zweck der Verarbeitung zusätzlich die Rechtsgrundlagen der Verarbeitung, allfällige Empfänger, die Dauer der Datenspeicherung, Hinweise auf die Betroffenenrechte sowie das Recht zur Beschwerde bei der Datenschutzbehörde zu nennen und ist über mögliche Folgen der Nichtbereitstellung der personenbezogenen Daten zu informieren. Die Informationen müssen vor oder zeitgleich mit der Erhebung der Daten erteilt werden. Bei Erhebungen auf einer Website können die Informationen im Rahmen einer Datenschutzerklärung erteilt werden.

Weiters bestehen Informationspflichten ferner dann, wenn personenbezogene Daten nicht bei den betroffenen Personen selbst, sondern auf andere Weise, etwa aus öffentlichen Quellen oder von Dritten, erhoben werden.

3. Auskunftsrecht

Nach Art 15 hat eine betroffene Person wie bisher das Recht auf Auskunft, ob und in welchem Ausmaß sie betreffende personenbezogene Daten von dem Verantwortlichen verarbeitet werden. Die betroffene Person hat auch das Recht auf Erhalt einer Kopie ihrer Daten, wobei die Rechte und Freiheiten anderer Personen hierdurch nicht beeinträchtigt werden dürfen.

Der Verantwortliche hat auch über die Speicherdauer Auskunft zu geben und auf das Recht auf Berichtigung, Löschung, Widerspruch und Einschränkung der Verarbeitung hinzuweisen. Ausnahmen vom Auskunftsrecht bestehen hinsichtlich der Offenbarung von Geschäfts- oder Berufsgeheimnissen und hinsichtlich des Schutzes geistigen Eigentums.

4. Recht auf Berichtigung und Löschung

Ähnlich wie bisher gewähren Art 16 und 17 DSGVO der betroffenen Person das Recht, unrichtige Daten richtigzustellen oder Daten löschen zu lassen. Der Verantwortliche ist verpflichtet, Daten auf Antrag eines Betroffenen sowie auch aus Eigenem zu löschen, wenn der Zweck der Verarbeitung wegfällt, wenn die Verarbeitung auf Grundlage einer Einwilligung erfolgte und diese widerrufen wird, wenn die betroffene Person erfolgreich Widerspruch erhoben hat, wenn die Daten unrechtmäßig verarbeitet wurden oder die Löschung aufgrund von gesetzlichen Verpflichtungen notwendig ist.

Ausnahmen von der Löschungspflicht bestehen ua zugunsten des Rechts auf Meinungs- und Informationsfreiheit, zugunsten im öffentlichen Interesse liegender Archivzwecke und wissenschaftlicher Forschungszwecke, bei gesetzlichen Aufbewahrungspflichten sowie zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

5. Recht auf Einschränkung

Das Recht auf Einschränkung (Art 18) ist als Begleitanspruch zu dem Recht auf Löschung, Berichtigung und Widerspruch zu sehen. Per definitionem handelt es um die "Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken".

6. Recht auf Datenübertragbarkeit

Gänzlich neu ist das Recht auf Datenübertragbarkeit (Art 20). Die betroffene Person hat das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen mitgeteilt hat, in einem "strukturierten, gängigen und maschinenlesbaren Format" zu erhalten oder an einen anderen Verantwortlichen übertragen zu lassen. Damit soll eine bessere Kontrolle über die eigenen Daten ermöglicht werden. Praktisch relevant ist dies in erster Linie für den Wechsel von Diensteanbietern.

Mögliche Anwendungsbeispiele sind die Übertragung von Musik-Wiedergabelisten beim Wechsel von Streaming-Diensten, E-Mails und Kontaktlisten beim Wechsel des Internetproviders oder Transaktionsdaten des Bankkontos beim Wechsel der Bank. Das Recht auf Datenübertragung besteht nur dann, wenn die Verarbeitung auf Grundlage einer Einwilligung oder eines Vertrags automatisiert erfolgt und wenn die Daten durch die betroffene Person bereitgestellt wurden.

7. Widerspruchsrecht

Das Widerspruchsrecht ermöglicht der betroffenen Person, **gegen rechtmäßige Verarbeitungen** personenbezogener Daten vorzugehen. Art 21 unterscheidet drei Fälle: Einerseits geht es um Verarbeitungen, die vom Verantwortlichen auf überwiegende berechtigte Interessen oder auf die Wahrnehmung einer Aufgabe im öffentlichen Interesse als Rechtsgrundlage gestützt werden. Die betroffene Person kann aus Gründen, die sich aus ihrer besonderen Situation ergeben, gegen derartige Verarbeitungen Widerspruch erheben. Die betroffene Person muss hierfür das Vorliegen einer **"besonderen Situation"** glaubhaft machen. In diesem Fall muss der Verantwortliche entweder zwingende schutzwürdige Gründe nachweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder nachweisen, dass die Verarbeitung der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen dient. Ferner gibt es ein gesondertes Widerspruchsrecht betreffend **Direktwerbung**. Hier ist ein Widerspruch jederzeit und auch ohne Begründung möglich. Bei einem Widerspruch dürfen die Daten nicht mehr für diesen Zweck verarbeitet werden. Es findet also keine weitere Interessenabwägung statt. Einen weiteren Spezialfall bildet der Widerspruch gegen eine Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken. In diesem Fall ist das Widerspruchsrecht nur begrenzt ausübbar.

8. Automatisierte Entscheidungen im Einzelfall und Profiling

Art 22 schützt den Betroffenen vor einer ausschließlich auf einer automatisierten Verarbeitung (einschl Profiling) beruhenden Entscheidung, die gegenüber der betroffenen Person **rechtliche Wirkung** entfaltet oder diese in ähnlicher Weise erheblich beeinträchtigt. Dadurch sollen Entscheidungen verhindert werden, die ohne menschliches Zutun getätigt werden.

Eine automatisierte Entscheidung ist ausnahmsweise erlaubt, wenn diese für den Abschluss eines Vertrags erforderlich ist, gesetzlich zulässig ist, oder eine ausdrückliche Einwilligung der betroffenen Person vorliegt.

9. Folgen eines Verstoßes gegen Betroffenenrechte

Verstöße gegen Betroffenenrechte können mit empfindlich hohen **Geldbußen** von bis zu 20 Mio Euro oder im Fall eines Unternehmens von bis zu 4 % des weltweit erzielten Jahresbruttoumsatzes sanktioniert werden. Die Geldbußen sollen wirksam, verhältnismäßig und abschreckend sein. Die Bemessung der Geldbuße richtet sich nach den Umständen des Einzelfalls, insb nach Art, Schwere und Dauer des Verstoßes, Schadenshöhe, Verschuldensgrad etc. Darüber hinaus hat jede betroffene Person das Recht auf Beschwerde bei der Aufsichtsbehörde und auf einen wirksamen gerichtlichen Rechtsbehelf.

RA Dr. Gerit Katrin Jantschgi, zert. DSBA der Gemeinde