# Information über datenschutzrechtliche Verpflichtungen als Mitglied in Gremien des Berliner Quartiersmanagements

Frau/Herr \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Sie erhalten im Rahmen Ihrer Tätigkeit als Mitglied des Quartiersrats/ der Aktionsfondsjury/ der Steuerungsrunde der Berliner Quartiersmanagements *XY* auch personenbezogene Daten zur Kenntnis. Sie werden daher auf die in Ihrer Verantwortung stehende gesetzliche Verpflichtung der Beachtung des Datenschutzes und der Vorgaben der Datenschutz-Grundverordnung in diesem Zusammenhang hingewiesen. Dies betrifft insbesondere die Wahrung der Vertraulichkeit der Ihnen im Rahmen Ihrer Aufgabenwahrnehmung bekannt gegebenen personenbezogenen Angaben.

Nach den Vorschriften der DSGVO ist es untersagt, personenbezogene Daten unbefugt oder unrechtmäßig zu verarbeiten oder absichtlich oder unabsichtlich die Sicherheit der Verarbeitung in einer Weise zu verletzen, die zur Vernichtung, zum Verlust, zur Veränderung, zur unbefugter Offenlegung oder unbefugtem Zugang führt.

Daher ist es Ihnen ausschließlich gestattet, personenbezogene Daten zweckgebunden im Rahmen der Ihnen übertragenen Aufgaben zu verarbeiten. Personenbezogene Daten dürfen nicht unbefugt anderen Personen mitgeteilt oder zugänglich gemacht werden oder von Ihnen selbst für andere Zwecke genutzt werden.

Diese Verpflichtungen bestehen umfassend und ohne zeitliche Begrenzung auch nach Beendigung Ihrer Tätigkeit als Mitglied in einem Gremium des Berliner Quartiersmanagements fort.

Verstöße gegen diese Verpflichtung können mit Geldbuße und/oder Freiheitsstrafe geahndet werden. Auch (zivilrechtliche) Schadenersatzansprüche können sich aus schuldhaften Verstößen gegen diese Verpflichtung ergeben.

Mit Ihrer Unterschrift erklären Sie, dass Sie

1. über Ihre Verpflichtungen nach der Datenschutz-Grundverordnung und die sich daraus ergebenden Verhaltensweisen unterrichtet wurden, insbesondere über den vertraulichen Umgang mit personenbezogenen Daten;
2. ein Exemplar dieser Information sowie ein Merkblatt mit dem Abdruck ausgewählter rechtlicher Vorschriften zum Datenschutz erhalten haben.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Ort, Datum Unterschrift der/des Verpflichteten

# Merkblatt zur Verpflichtungserklärung

Die vorliegende Auswahl gesetzlicher Vorschriften soll Ihnen einen Überblick über das datenschutzrechtliche Regelwerk verschaffen. Die Darstellung erfolgt exemplarisch und erhebt keinen Anspruch auf Vollständigkeit. Weitere Informationen zu datenschutzrechtlichen Fragestellungen erhalten Sie bei der Berliner Beauftragten für Datenschutz und Informationsfreiheit.

**Aufgaben des Quartiersrats und der Aktionsfondsjurys**

§ 171e Abs. 5 BauGB: Bei der Erstellung des Entwicklungskonzeptes und bei seiner Umsetzung sollen die Beteiligten **in geeigneter Form einbezogen und zur Mitwirkung angeregt** werden.

Art. 9 Abs. 1 VV Städtebauförderung 2020: Zur stärkeren Beteiligung und Mitwirkung von Betroffenen kann die Gemeinde einen Fonds einrichten, über die **Verwendung dessen Mittel entscheidet ein lokales Gremium** (Verfügungsfonds).

4.1 VV SoZus 2021: Vorhaben werden nur gefördert, wenn sie mit dem Integrierten Handlungs- und Entwicklungskonzept (IHEK, Konzept gemäß § 171e Abs. 4 des Baugesetzbuches (BauGB)) im Einklang stehen und die lokalen Bürgergremien (Aktionsfondsjury, Quartiersrat) und die Steuerungsrunde die **Übereinstimmung der Projektinhalte mit den Zielen des IHEK** festgestellt haben.

VfG Aktionsfonds 2021: Das QM-Team legt alle förderfähigen Anträge der Aktionsfondsjury vor. Diese entscheidet anhand der **Förderwürdigkeit darüber, welche Aktionen gefördert** werden.

VfG Projektfonds 2021: Unter den förderfähigen Anträgen wird der am besten geeignete durch ein **Auswahlgremium ausgewählt**. Die Steuerungsrunde bestimmt dessen Mitglieder; der Quartiersrat kann Vertreter benennen.

**Begrifflichkeiten**

Art. 4 Nr. 1 DS-GVO: **„Personenbezogene Daten“** [sind] alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

Art. 4 Nr. 2 DS-GVO: **„Verarbeitung“** [meint] jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

**Grundsätze der Verarbeitung**

Art. 5 Abs. 1 lit. a DS-GVO: Personenbezogene Daten müssen […] auf **rechtmäßige Weise,** nach Treu und Glauben und in einer für die betroffene Person **nachvollziehbaren Weise** verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“).

Art. 5 Abs. 1 lit. f DS-GVO: Personenbezogene Daten müssen […] in einer Weise verarbeitet werden, die eine angemessene **Sicherheit** der personenbezogenen Daten gewährleistet, einschließlich Schutz vor **unbefugter oder unrechtmäßiger Verarbeitung** und vor unbeabsichtigtem **Verlust**, unbeabsichtigter **Zerstörung** oder unbeabsichtigter **Schädigung** durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“).

Art. 32 Abs. 2 DS-GVO: Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung – insbesondere durch **Vernichtung, Verlust** oder **Veränderung**, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte **Offenlegung** von beziehungsweise unbefugten **Zugang** zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind.

Art. 33 Abs. 1 Satz 1 DS-GVO: Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der […] zuständigen Aufsichtsbehörde, es sei denn, dass die **Verletzung** des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

**Haftung**

Art. 82 Abs. 1 DS-GVO: Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf **Schadenersatz** gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.

Art. 83 Abs. 1 DS-GVO: Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von **Geldbußen** gemäß diesem Artikel für Verstöße gegen diese Verordnung […] in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.

§ 42 BDSG-neu (1) Mit **Freiheitsstrafe** bis zu drei Jahren oder mit **Geldstrafe** wird bestraft, wer wissentlich nicht allgemein zugängliche personenbezogene Daten einer großen Zahl von Personen, ohne hierzu berechtigt zu sein,

1. einem Dritten übermittelt oder
2. auf andere Art und Weise zugänglich macht

und hierbei gewerbsmäßig handelt.

(2) Mit **Freiheitsstrafe** bis zu zwei Jahren oder mit **Geldstrafe** wird bestraft, wer personenbezogene Daten, die nicht allgemein zugänglich sind,

1. ohne hierzu berechtigt zu sein, verarbeitet

oder

1. durch unrichtige Angaben erschleicht

und hierbei gegen Entgelt oder in der Absicht handelt, sich oder einen anderen zu bereichern oder einen anderen zu schädigen.

§ 202a Abs. 1 StGB: Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit **Freiheitsstrafe** bis zu drei Jahren oder mit **Geldstrafe** bestraft.

§ 303a Abs. 1 StGB: Wer rechtswidrig Daten […] löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit **Freiheitsstrafe** bis zu zwei Jahren oder mit **Geldstrafe** bestraft.