Datenschutz-Leitlinien

Anlage 3

für die ARGE U-Bahn Nürnberg U3 SW BA 2.2

INHALTSVERZEICHNIS

1 Anwendungsbereich und Ziele zum Schutz von Personendaten

1.1 Wesentliche Grundbegriffe

„**personenbezogene Daten**“ sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (z.B. Name, Kontaktdaten, IP-Adresse, Standort-Daten, Geschlecht, Geburtsdatum, Ton- und Bildaufnahmen);

„**Besondere Kategorien personenbezogener Daten**“ sind personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person (z.B. Lichtbild, nur wenn es mit speziellen technischen Mitteln verarbeitet wird, die die eindeutige Identifizierung ermöglichen), Gesundheitsdaten, Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person;

„**Verarbeitung**“ ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführter Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

„**Verantwortlicher**“ ist die natürliche oder juristische Person oder Behörde, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet;

„**Auftragsverarbeiter**“ ist eine natürliche oder juristische Person oder Behörde, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;

1.2 Datenschutzziele

Im Rahmen der Tätigkeit der Arbeitsgemeinschaft fallen personenbezogene Daten an. Zum einen sind dies die Daten von Personen (z.B. Kontaktdaten von Lieferanten und Kunden sowie von Mitarbeitern der Arbeitsgemeinschaft und deren Gesellschaftern). Diese Daten wollen wir nach den geltenden Datenschutzgesetzen verarbeiten und vor unberechtigten Zugriffen durch geeignete technische und organisatorische Maßnahmen schützen.

2 Grundsätze für die Verarbeitung personenbezogener Daten

2.1 Rechtmäßigkeit der Verarbeitung

Ein wesentlicher Grundsatz ist das so genannte **Verbotsprinzip mit Erlaubnisvorbehalt**. Dieses besagt, dass die Verarbeitung von personenbezogenen Daten im Prinzip verboten ist und nur zulässig ist, wenn dies gesetzlich erlaubt ist. Es gibt die nachfolgend aufgezählten Rechtmäßigkeitsgrundlagen, auf die eine Verarbeitung gestützt werden kann, **wobei im Grundsatz eine Einwilligung als letztes Mittel ausgeschöpft werden sollte, wenn nicht bereits eine andere Rechtsgrundlage einschlägig ist. In vielen Fällen wird die Verarbeitung auf die Verarbeitung zur Erfüllung eines Vertrages oder auf überwiegende berechtigte Interessen gestützt werden können**.

Die Verarbeitung **besonderer Kategorien personenbezogener Daten** (siehe Ziff. 1.1) ist nach Art. 9 DSGVO jedoch stärker eingeschränkt, so dass nicht alle nachstehenden Erlaubnisvorbehalte greifen und insbesondere eine Verarbeitung auf überwiegende berechtigte Interessen nicht gestützt werden kann.

2.1.1.1 Verarbeitung zur Erfüllung eines Vertrages mit dem Betroffenen

Die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen.

Personenbezogene Daten von Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung oder zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist.

2.1.1.2 Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung

Die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt. Hier finden sich Rechtsgrundlagen vor allem im Betriebsverfassungsrecht bei der betrieblichen Mitbestimmung sowie im Sozialversicherungs- und Steuerrecht.

2.1.1.3 Verarbeitung zum Schutz lebenswichtiger Interessen

Die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen (z.B. im Rahmen eines Arbeitsunfalles).

2.1.1.4 Verarbeitung für eine Aufgabe im öffentlichen Interesse

Die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.

2.1.1.5 Verarbeitung aufgrund überwiegender berechtigter Interessen

Die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Die betroffene Person hat jedoch das Recht, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten **Widerspruch einzulegen**. Zudem muss die betroffene Person spätestens zum Zeitpunkt der ersten Kommunikation mit ihr ausdrücklich auf das Widerspruchsrecht **hingewiesen** werden. dieser Hinweis hat in einer verständlichen und von anderen Informationen getrennter Form zu erfolgen und ist am besten mit den Informationspflichten (s.u. Ziff. 3.2.4) zu verbinden.

2.1.1.6 Verarbeitung aufgrund Tarifvertrag / Betriebsvereinbarung

Die Verarbeitung personenbezogener Daten, einschließlich besonderer Kategorien personenbezogener Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses, ist auf der Grundlage von Kollektivvereinbarungen (Tarifvertrag / Betriebsvereinbarung) zulässig.

2.1.1.7 Verarbeitung aufgrund Einwilligung

Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben. Bei der Dokumentation der Einwilligung sind folgende Punkte zu beachten:

- Das Ersuchen um Einwilligung muss in leicht verständlicher Form und Sprache erfolgen und muss von anderen Sachverhalten klar zu unterscheiden sein (ggf. eigener Kasten / separate Unterschrift).
- Belehrung über Widerrufsrecht vor Abgabe der Einwilligungserklärung. Der Widerruf muss so einfach wie die Erteilung der Einwilligung sein.
- Das Ersuchen um Einwilligung mit der Belehrung über das Widerrufsrecht ist am besten mit den Informationspflichten (s.u. Ziff. 3.2.4) zu verbinden.
- Die Einwilligung muss zudem freiwillig erteilt worden sein. Bei der Beurteilung der Freiwilligkeit der Einwilligung insbesondere die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Person sowie die Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen.
- Bei Kindern unter 16 Jahren ist die Dokumentation der Einwilligung der personensorgeberechtigten Eltern erforderlich (wenn ein Rechtsgeschäft betroffen ist, auch noch bis 18 Jahre) und bei Einsichtsfähigkeit des Kindes ab etwa 14 Jahren evtl. auch die Einwilligung des Kindes, wenn dessen Persönlichkeitsrecht (z.B. Bildrechte) betroffen ist.
- Aufgrund der Nachweispflicht des Verantwortlichen wird die Einwilligung am besten in Textform (z.B. Email) oder in Schriftform dokumentiert. Im Beschäftigungsverhältnis bedarf die Einwilligung der Schriftform (mit Originalunterschrift), soweit nicht wegen besonderer Umstände eine andere Form angemessen ist.

2.2 Zweckbindungsgrundsatz

Personendaten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. Zu unterschiedlichen Zwecken erhobene Daten müssen getrennt verarbeitet werden.

Zweckänderungen sind nur dann möglich, wenn eine Rechtsvorschrift die Zweckänderung erlaubt, eine Einwilligung des Betroffenen hierzu vorliegt oder der Zweck der weitergehenden Verarbeitung mit dem ursprünglichen Zweck der Datenerhebung vereinbar ist (Kompatibilitätstest § 6 Abs. 4 DSGVO).

2.3 Datenminimierung, Datenrichtigkeit

Personendaten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein (**Privacy by Design** und **Privacy by Default** – z.B. Datenschutzfreundliche Voreinstellung der Software-Systeme).

Von den Möglichkeiten der **Anonymisierung** (keine Zuordnung zu einer Person mehr möglich) und **Pseudonymisierung** (Zuordnung mit Hilfsmitteln noch möglich) ist Gebrauch zu machen, soweit der Umsetzungsaufwand verhältnismäßig ist.

Unrichtige Daten sind zu **berichtigen bzw. zu löschen**.

2.4 Speicherbegrenzung

Personenbezogene Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Personendaten sind nach Ablauf der Erforderlichkeit zu **löschen**, wenn es keine anderen gesetzlichen Pflichten zur weiteren Aufbewahrung der Daten insbesondere hinsichtlich handels- und steuerrechtlicher Aufbewahrungsfristen (bis zu 10 Jahre) gibt, die Daten zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen im Rahmen der geltenden Verjährungsvorschriften (bis zu 30 Jahre) notwendig sind oder ein berechtigtes Interesse des Verantwortlichen besteht.

Alle für die Abrechnung der Arge erforderlichen Daten sowie für den Nachweis der ordnungsgemäßen Leistungserbringung relevante Leistungsdaten (einschließlich der Unterlagen zur Abwicklung von Nachunternehmer-Vertragsverhältnissen) werden mit Abschluss

der ARGE zur Speicherung und Aufbewahrung an die jeweiligen Gesellschafter übergeben. Jeder Gesellschafter hat sicherzustellen, dass die übergebenen Daten nach Ablauf der Aufbewahrungsfristen gelöscht werden. Für abrechnungsrelevante Daten wird eine Standard-Löschfrist von 13 Jahren beginnend mit Abnahme der Arge-Leistungen geregelt. Haftungsrelevante Daten werden mit einer Standard-Löschfrist von 33 Jahren nach Abnahme der Arge-Leistungen belegt.

Sonstige personenbezogene Daten sind nach Ablauf der Erforderlichkeit zu löschen. Entsprechende Regeln zur Archivierung und Löschung von Personendaten dieser sonstigen Daten sind in der ARGE zu identifizieren und festzulegen.

2.5 Integrität und Vertraulichkeit

Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine **dem Risiko angemessene Sicherheit** der personenbezogenen Daten durch **geeignete technische und organisatorische Maßnahmen** gewährleistet (siehe hierzu nachstehend Ziff. 3 – Technische und organisatorische Maßnahmen).

3 Technische und organisatorische Maßnahmen (TOM)

3.1 Grundsätze

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen **Eintrittswahrscheinlichkeit und Schwere des Risikos** für die Rechte und Freiheiten natürlicher Personen sind geeignete technische und organisatorische Maßnahmen zu treffen, um ein **dem Risiko angemessenes Schutzniveau** zu gewährleisten. Der Verantwortliche hat hierbei die einschlägigen Technischen Richtlinien und Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik zu berücksichtigen. Diese Maßnahmen schließen unter anderem Folgendes ein

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Im Fall einer **automatisierten Verarbeitung** sind nach einer **Risikobewertung** Maßnahmen zu ergreifen, die Folgendes bezwecken:

- Zugangskontrolle: Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte,
- Datenträgerkontrolle: Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern,
- Speicherkontrolle: Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten,
- Benutzerkontrolle: Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte,
- Zugriffskontrolle: Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben,

- Übertragungskontrolle: Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können,
- Eingabekontrolle: Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind,
- Transportkontrolle: Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden,
- Wiederherstellbarkeit: Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können
- Zuverlässigkeit: Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden,
- Datenintegrität: Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können,
- Auftragskontrolle: Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können,
- Verfügbarkeitskontrolle: Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind,
- Trennbarkeit: Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können.
- Belastbarkeit: Widerstandsfähigkeit der IT im Fehlerfall, bei Störungen, bei hoher Beanspruchung – z.B. DoS-Attacken

3.2 Technische und organisatorische Maßnahmen der Arbeitsgemeinschaft

3.2.1 Verzeichnis der Verarbeitungstätigkeiten

Für die Tätigkeiten im Rahmen der Arbeitsgemeinschaft wird ein Verzeichnis von Verarbeitungstätigkeiten erstellt und regelmäßig vom Datenschutzkoordinator aktualisiert, in welchem alle Verarbeitungstätigkeiten zu Personendaten im Rahmen der Arge-Tätigkeit gelistet sind. Das Verzeichnis sowie Aktualisierungen sind den Gesellschaftern der ARGE unverzüglich zur Verfügung zu stellen, damit die Gesellschafter ihre eigenen Verarbeitungsverzeichnisse hiermit abstimmen können.

3.2.2 Verpflichtung auf den Datenschutz

Das ggf. in der ARGE angestellte Personal wird gemäß dem Muster in **Anlage A** auf den Datenschutz verpflichtet. Der Datenschutzkoordinator ist für die Dokumentation der Verpflichtungen verantwortlich. Jeder Gesellschafter der ARGE, der an die ARGE Personal abstellt, ist verpflichtet, die abgestellten Personen entsprechend zu verpflichten.

3.2.3 Auftragsverarbeiter

Eine Auftragsverarbeitung im datenschutzrechtlichen Sinne liegt nur in Fällen vor, in denen eine Stelle von einem Verantwortlichen im Schwerpunkt mit der Verarbeitung personenbezogener Daten nach den Weisungen des Verantwortlichen beauftragt wird.

Die Beauftragung mit fachlichen Dienstleistungen, bei denen nicht die Personendatenverarbeitung im Vordergrund steht bzw. einen wichtigen Kernbestandteil ausmacht, stellt keine Auftragsverarbeitung im datenschutzrechtlichen Sinne dar (z.B. Inkassobüros, Bank für Geldtransfer, Personalvermittlung, Schulungstrainer, Druck von Prospekten mit Personenbildern).

Die Arbeitsgemeinschaft sowie deren Gesellschafter dürfen im Rahmen der Arbeitsgemeinschaft nur mit Auftragsverarbeitern zusammenarbeiten, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit dem Datenschutzrecht stehen. Hierzu ist eine

Vereinbarung mit dem gesetzlich vorgeschriebenen Inhalt zu schließen, wozu das Muster in **Anlage B** verwendet werden kann.

3.2.4 Informationspflichten bei Direkt- oder Dritterhebung

Sobald personenbezogene Daten bei einer betroffenen Person erhoben werden, so hat der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten die in Art. 13 DSGVO aufgelisteten Angaben zu machen. Werden die Personendaten bei einem Dritten erhoben, so ist die betroffene Person nach Art. 14 DSGVO innerhalb einer angemessenen Frist jedoch spätestens zum Zeitpunkt der ersten Mitteilung an die Person über die Angaben zu informieren.

Die Angabepflichten umfassen Name/Kontaktdaten des Verantwortlichen, Kontaktdaten des Datenschutzbeauftragten, die Verarbeitungszwecke, die betroffenen Kategorien personenbezogener Daten, die Empfänger/Empfängerkategorien der Personendaten, ggf. die Absicht der Übermittlung in ein Drittland, die Dauer der Speicherung, ggf. die berechtigten Interessen, auf denen Verarbeitung beruht und die Betroffenenrechte.

Entsprechende Muster zur Erfüllung der Informationspflichten (z.B. Datenschutzhinweise für die Internetseite, Datenschutzhinweise an Mitglieder) werden verwendet.

3.2.5 Veröffentlichung von Personenbildern

- Wird für Aufnahmen von Personen ein externer Fotograf/Filmer beauftragt, ist mit diesem zusätzlich zum Dienst-/oder Werkvertrag eine Auftragsverarbeitungsvereinbarung zu schließen. Für Aufnahmen durch Pressevertreter ist die Presse grundsätzlich selbst und im Eigeninteresse verantwortlich – ein Auftragsverhältnis zur Presse bzw. auch ein Nutzungsrecht an dem Material der Presse wird im Regelfall nicht bestehen.
- Für Aufnahmen von öffentlichen Veranstaltungen, die die Veranstaltung als solche charakterisieren und nicht eine Einzelperson in den Fokus nehmen (Aufnahmen von der Veranstaltung in der Totalen und großen Gruppen, bei denen die einzelne Person vor dem eingefangenen Gesamteindruck der Veranstaltung zurücktreten also Beiwerk sind bzw. Einzelaufnahmen von Personen, die einem zentralen Veranstaltungszweck nachgehen, wie z. B. Vortragende oder Musikgruppen), wird keine Einwilligung der betroffenen Personen benötigt bzw. die Einholung von Einwilligungen von allen Personen wäre auch nicht praktikabel und mit weiteren Problemstellungen insbesondere im Falle des Widerrufs verknüpft. Auch soweit Personen der Zeitgeschichte abgelichtet sind, wird keine Einwilligung in Bildaufnahmen bei einer Veranstaltung benötigt.
- Bei Aufnahmen von Einzelpersonen/kleineren Gruppen, die einzelne Personen charakterisieren, die keine Person der Zeitgeschichte sind, bzw. wenn Personen z.B. in ihrer Intimsphäre betroffen sind, sollte eine Einwilligung, die auch konkludent durch schlüssiges Handeln erteilt werden kann, dokumentiert werden und soweit sinnvoll sogar schriftlich dokumentiert werden. Bei Verwendung eines Einwilligungsformulars sollte dieses auch die Datenschutzhinweise nach Art. 13 DSGVO bereits beinhalten. Bei Minderjährigen unter 18 Jahren ist auf die Einwilligung des Kindes (sofern das Kind mindestens 14 Jahre alt ist) sowie auf die Einwilligung der sorgeberechtigten Eltern zu achten.
- Widerruft eine betroffene Person die erteilte Einwilligung später oder – wenn die Aufnahme auf ein vorrangiges berechtigtes Interesse gestützt wird – widerspricht die betroffene Person der Publikation der Aufnahme, muss geprüft werden, inwieweit die Anpassung der Publikation einfach möglich ist oder die Nichtveränderung der Publikation auf schutzwürdige Gründe gestützt werden kann.

3.2.6 Datenübermittlung in Drittländer

Eine Datenübermittlung in Drittländer findet nicht statt.

3.2.7 Technische Datensicherheit

Die technische Datensicherheit wird u. a. durch eine Verschlüsselung der zur Speicherung der Daten verwendeten Medien, Schutz der Speichermedien durch Passwörter, Schutz der in den Geschäftsräumen installierten Rechnern mit Passwörtern erreicht. Daten werden in regelmäßigen Abständen gesichert und verschlossen zur Sicherung aufbewahrt.

4 Umgang mit Betroffenenrechten / Datenschutzverletzungen

4.1 Betroffenenrechte

Neben der Informationspflicht des Verantwortlichen (s.o. Ziff. 3.2.4) und dem Recht eine erteilte Einwilligung zu widerrufen (s.o. Ziff. 2.1.1.7) stehen betroffenen Personen das Recht auf Auskunft (Art. 15 DSGVO, §§ 34, 35 BDSG), das Recht auf Berichtigung (Art. 16 DSGVO), das Recht auf Löschung (Art. 17 DSGVO, §§ 34, 35 BDSG), das Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO), das Widerspruchsrecht gegen die Verarbeitung (Art. 21 DSGVO) und das Recht auf Datenübertragbarkeit (Art. 20 DSGVO) zu. Es besteht zudem die Möglichkeit, sich mit einer Beschwerde an eine Datenschutzaufsichtsbehörde zu wenden.

Macht eine betroffene Person diese Rechte geltend, ist der Datenschutzkoordinator der Arbeitsgemeinschaft zu informieren und in Abstimmung mit diesem entsprechend den gesetzlichen Anforderungen auf das Begehren der betroffenen Person zu reagieren.

4.2 Datenschutzverletzungen

4.2.1 Meldepflicht gegenüber Aufsichtsbehörde

Eine Verletzung des Schutzes personenbezogener Daten ist eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von bzw. zum unbefugten Zugang zu personenbezogenen Daten führt, die verarbeitet wurden.

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**.

4.2.2 Benachrichtigung der betroffenen Person

Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt der Verantwortliche die betroffene Person unverzüglich von der Verletzung.