STADTQUARTIER 2050:

Herausforderungen gemeinsam lösen

Partner:

Assoziierte Partner:

Deliverable D3.1.1

Datenschutz- und Datensicherheitskonzept des öffentlich geförderten Projekts

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Erstellt im Verbundvorhaben STADTQUARTIER 2050 im Rahmen der Förderinitiative „Solares Bauen/ Energieeffiziente Stadt“ aus dem 6. Energieforschungs-programm

Autoren:

Marco Schmidt, Dominic Stirnweiß, Fraunhofer FIT

Gefördert durch:
Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

Augsburg, 31.10.2018

Version 1.0

Inhalt

1 Einführung

Seit März 2018 fördern die Bundesministerien für Bildung und Forschung sowie Wirtschaft und Energie das Projekt „STADTQUARTIER 2050 - Herausforderungen gemeinsam lösen: Beispielgebende Sanierung und Nachverdichtung von Stadtquartieren zu klimaneutralen Wohnsiedlungen mit Leuchtturmanwendungen in Stuttgart und Überlingen“. Das Projektkonsortium besteht auf der Seite der Wissenschaft aus der Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e. V., der Universität Stuttgart, dem Institut für Ressourceneffizienz und Energiestrategien GmbH sowie dem Forschungsinstitut für Wärmeschutz e. V. München, auf der Seite der Kommunen aus der Landeshauptstadt Stuttgart sowie der Stadt Überlingen und auf der Seite der Wirtschaft aus der Baugenossenschaft Überlingen eG, der Stadtwerke Stuttgart GmbH, der Stadtwerk am See GmbH & Co. KG, der Energieagentur Ravensburg gGmbH, der IBS Ingenieurbüro Schuler GmbH sowie der puren GmbH.

1.1 Projekthintergrund und Ziele

Im Rahmen des Projekts STADTQUARTIER 2050 soll in den beiden Städten Stuttgart und Überlingen je ein Quartier entstehen, das eine klimaneutrale Energieversorgung sowie einen hohen energetischen Standard bei gleichzeitig bezahlbaren Mieten erreicht. Insgesamt entstehen in beiden Quartieren 960 Wohneinheiten in teils neu zu errichtenden Gebäuden, teils zu sanierenden Bestandsgebäuden. Dabei soll modernste Technologie aus den Bereichen Photovoltaik, Geothermie, Wärmeschutz und Elektromobilität zum Einsatz kommen. Ein selbstlernender Steuerungsmechanismus („Grid Optimizer“) prognostiziert den Energiebedarf und optimiert die Nutzung von solarem Strom im Quartier. Darüber hinaus wird untersucht, wie Bewohner mithilfe von app-basiertem Feedback („Quartiers-App“) sowie einem Belohnungssystem zur Mitarbeit am gemeinsamen Ziel der Energieeffizienz aktiviert werden können.

Um die Erreichung der Klimaneutralitäts- und Energieeffizienzziele im Quartier zu überprüfen, sind detaillierte Informationen über die Energienutzung auf Gebäudeebene notwendig. Grid Optimizer und Quartiers-App benötigen darüber hinaus fein aufgelöste Verbrauchsdaten auf Wohnungsebene. Zusätzlich soll die Wirksamkeit der Feedback- und Belohnungsmaßnahmen mithilfe von Befragungen erfasst werden, die demographische Daten zu den Bewohnern enthalten. Deshalb besteht eine der zentralen Herausforderungen des Projekts in der Umsetzung von gesetzlichen Vorgaben im Bereich Datenschutz und -sicherheit dieser Daten.

1.2 Datensatz

Der in diesem Konzept betrachtete Datensatz dient unterschiedlichen Zwecken, die in D3.1.2 Use Cases näher erläutert werden. Auf Quartiers-, Haus- und Wohnungsebene werden Energieverbrauchsdaten erhoben, um zum einen die Erreichung der Klimaneutralitäts- und Energieeffizienzziele zu überprüfen und zum anderen, um den Bewohnern Feedback zu ihrem Verbrauch und Anreize zur Energieeinsparung zu geben. Neben Strom-, Wärme- und Warmwasserverbrauchsdaten müssen auf Wohnungsebene zusätzliche Daten zur Wohnung, den Bewohnern und deren Wohnverhalten erhoben werden. Dazu gehören Wohnklimadaten (z. B. Luftfeuchtigkeit, Raumtemperatur), Bewohnerdaten (z. B. Anzahl Bewohner, Alter der Bewohner, Beschäftigungsstatus, tägliche Anwesenheitszeiten, Ökologiebewusstsein, Anzahl an Elektrogeräten) sowie die Lage der Wohnung innerhalb eines Quartiers (z. B. Stockwerk). Tabelle 1 listet die zu erhebenden Daten, die relevanten Betrachtungsebenen sowie eine mögliche zeitliche Auflösung auf und referenziert die dazugehörigen Datennutzungszwecke aus D3.1.2. Die Auflösung, mit der die Daten erhoben werden, hängt von der eingesetzten Messtechnik (z. B. Smart Meter) ab und kann bei Bedarf während des Betriebs angepasst werden.

1.3 Geltungsbereich und Stand des Konzepts

Dieses Konzept soll alle Aspekte des Datenschutzes und der Datensicherheit abdecken, die sich direkt aus der Erfassung, Speicherung und Verarbeitung der genannten Daten während der Laufzeit des Projekts ergeben. Nicht abgedeckt sind Bestimmungen und Aktivitäten über den Projektzeitraum hinaus sowie Details zur Umsetzung innerhalb einzelner Artefakte wie Quartiers-App oder Grid Optimizer.

Dieses Dokument beinhaltet sowohl konkrete Instrumente zur Sicherstellung des Datenschutzes und der Datensicherheit im Projekt als auch allgemeine handlungsleitende Prinzipien mit Rechten und Pflichten, die im Zusammenhang mit der Erfassung, Speicherung und Verarbeitung der genannten Daten stehen. Die vorliegende Version spiegelt den Stand des Konzepts zum genannten Erstellungsdatum wieder. Viele Entscheidungen zu Designalternativen und Rahmenbedingungen sind noch nicht gefallen und im Vorfeld nicht absehbar. Deshalb wird das Konzept in regelmäßigen Abständen aktualisiert und erweitert.

1.4 Verpflichtung zum Datenschutz

Alle Personen, die bei der Verarbeitung von im Projekt SQ2050 erhobenen Daten beteiligt sind, verpflichten sich den in diesem Konzept festgehaltenen

Datenschutzkriterien. Mitarbeiter der beteiligten Projektpartner, die mit der Verarbeitung von Daten in Berührung kommen, sind bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten bzw. darüber zu unterrichten. Die Verpflichtung zur Wahrung des Datengeheimnisses bleibt auch über den Zeitraum ihrer Tätigkeit hinaus bestehen.

Tabelle 1. Übersicht der erhobenen Daten aus D4.3.2 Use Cases

Datentyp	**erhobene Daten**	**Betrachtungsebene**	**Auflösung**	**Use Cases (siehe D4.3.2)**
Verbrauchsdaten	Stromverbrauch	• Quartier • Haus • Wohnung	<1 min	Energiebedarfsprofile (UC1), Grid Optimizer (UC2), Quartiers-App (UC4, UC5), Belohnungssystem (UC3), Forschungsaktivitäten (UC6)
	Wärmeverbrauch	• Quartier • Haus • Wohnung	5-60 min	Energiebedarfsprofile (UC1), Grid Optimizer (UC2), Quartiers-App (UC4, UC5), Belohnungssystem (UC3), Forschungsaktivitäten (UC6)
	Warmwasserverbrauch	• Quartier • Haus • Wohnung	5-60 min	Energiebedarfsprofile (UC1), Grid Optimizer (UC2), Quartiers-App (UC4, UC5), Belohnungssystem (UC3), Forschungsaktivitäten (UC6)
Wohnklimadaten	Raumtemperatur, Luftfeuchtigkeit	• Wohnung	5-60 min	Quartiers-App (UC5), Belohnungssystem (UC3), Forschungsaktivitäten (UC6)
Bewohnerdaten	Demographie (Anzahl Personen, Alter, Beschäftigungsverhältnisse, Einkommen, Anwesenheitszeiten)	• Wohnung	einmalig	Energiebedarfsprofile (UC1), Quartiers-App (UC5), Forschungsaktivitäten (UC6)
	Ökologiebewusstsein	• Wohnung	monatlich	Quartiers-App (UC5), Forschungsaktivitäten (UC6)
	Wohlfühltemperatur, Lüftungsverhalten, Heizverhalten	• Wohnung	monatlich	Quartiers-App (UC5), Forschungsaktivitäten (UC6)
	Vorhandene Elektrogeräte	• Wohnung	halbjährlich	Grid Optimizer (UC2), Quartiers-App (UC5), Forschungsaktivitäten (UC6)
Wohnungsstammdaten	Lage im Quartier (Stockwerk)	• Wohnung	einmalig	Energiebedarfsprofile (UC1), Quartiers-App (UC5), Forschungsaktivitäten (UC6)
Umgebungsdaten	Wetter	• Quartier	5-60 min	Grid Optimizer (UC2), Quartiers-App (UC5), Belohnungssystem (UC3), Forschungsaktivitäten (UC6)

2 Rechtliche Rahmenbedingungen

Grundlage für das hier vorliegende Datenschutzkonzept ist die im Mai 2018 in der EU in Kraft getretene Datenschutzgrundverordnung (DSGVO). Diese gilt auf nationaler Ebene für alle EU-Mitgliedsstaaten und gilt für alle Informationen zu identifizierbaren oder identifizierten Personen (Erwägungsgrund 026 DSGVO 2018). Durch die Neufassung des Bundesdatenschutzgesetzes (BDSG) werden nationale Regelungen zum Datenschutz mit den Öffnungsklauseln der DSGVO vereint und somit auch die nationalen Interessen bzgl. Datenschutz gewahrt (DSGVO 2018).

2.1 Grundbegriffe

Um das Projektvorhaben umzusetzen, werden verschiedene Daten benötigt (Tabelle 1), die mittels automatisierter Verfahren (z. B. Smart-Meter-Technik, Strom- und Wärmezähler) oder manuell (z. B. papierbasierter Fragebogen) erhoben, gespeichert und verarbeitet werden (Monitoring- und Steuerungseinheit, Quartiers-App, Grid Optimizer). Dazu gehören u. a. Daten zu Bewohnern der Quartiere (Betroffener) und Informationen über deren spezifische Gewohnheiten sowie Daten zur Lage der Wohnung innerhalb eines Quartiers (z. B. Stockwerk, Gebäudeseite). Mitunter lassen sich aus diesen Daten Rückschlüsse auf einzelne Personen in den Quartieren ziehen, so dass diese als personenbezogen anzusehen sind und unter einen besonderen Schutz nach Datenschutzrecht fallen (Art. 4 DSGVO 2018):

> Artikel 4 DSGVO Absatz (1): Personenbezogene Daten
>
> *„Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche 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, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.“*

Personenbezogene Daten sind bei der Verarbeitung besonders zu schützen, wobei nach Artikel 4 Absatz 2 (Art. 4 DSGVO 2018) unter *Verarbeitung personenbezogener Daten* folgendes zu verstehen ist:

Art. 4 DSGVO Absatz (2): Verarbeitung personenbezogener Daten

„Unter „Verarbeitung versteht man jedes mit oder ohne Hilfe automatisierte Verfahren, jeden 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 von Daten.“

Demnach müssen personenbezogene Daten nach (Art. 5 DSGVO 2018)

- 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“)
- für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken („Zweckbindung“)
- dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“)
- sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“)
- 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; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden („Speicherbegrenzung“)
- 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“)

Die Verarbeitung personenbezogener Daten wird zusätzlich durch Artikel 89 (Art. 89 DSGVO 2018) sowie §27 (§ 27 BDSG 2018) geregelt. Demnach sind bestimmte Rechte der Betroffenen eingeschränkt, wenn personenbezogene Daten für statistische und wissenschaftliche Zwecke erhoben werden (sogenanntes „Wissenschaftsprivileg“). Diese Artikel kommen im Forschungsprojekt STADTQUARTIER 2050 zur Geltung, sodass die Schuttziele „Zweckbindung“ und „Speicherbegrenzung“ etwas geöffnet werden, um wissenschaftliche Erkenntnisse zu ermöglichen. Nichtsdestotrotz ist darauf zu achten, dass zukünftige Bewohner der Quartiere über die Art der Datenerhebung, deren Speicherung und deren Verarbeitung korrekt informiert werden und die Erlaubnis zur Verarbeitung eingeholt wird. Grundsätzlich sollten die Daten auch nur für die vorgesehenen Zwecke verwendet werden. Abweichungen vom vorgesehenen Verwendungszweck sind jedoch möglich.

§27 BDSG: Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken

(1) Abweichend von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 auch ohne Einwilligung für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke zulässig, wenn die Verarbeitung zu diesen Zwecken erforderlich ist und die Interessen des Verantwortlichen an der Verarbeitung die Interessen der betroffenen Person an einem Ausschluss der Verarbeitung erheblich überwiegen. Der Verantwortliche sieht angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person gemäß § 22 Absatz 2 Satz 2 vor.

(2) Die in den Artikeln 15 (Auskunftsrecht), 16 (Recht auf Berichtigung), 18 (Recht auf Einschränkung der Verarbeitung) und 21 (Widerspruchsrecht) der Verordnung (EU) 2016/679 vorgesehenen Rechte der betroffenen Person sind insoweit beschränkt, als diese Rechte voraussichtlich die Verwirklichung der Forschungs- oder Statistikzwecke unmöglich machen oder ernsthaft beinträchtigen und die Beschränkung für die Erfüllung der Forschungs- oder Statistikzwecke notwendig ist. Das Recht auf Auskunft gemäß Artikel 15 der Verordnung (EU) 2016/679 besteht darüber hinaus nicht, wenn die Daten für Zwecke der wissenschaftlichen Forschung erforderlich sind und die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde.

(2) Ergänzend zu den in § 22 Absatz 2 genannten Maßnahmen sind zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken verarbeitete besondere Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 zu anonymisieren, sobald dies nach dem Forschungs- oder Statistikzweck möglich ist, es sei denn, berechtigte Interessen der betroffenen Person stehen dem entgegen. Bis dahin sind die Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person zugeordnet werden können. Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Forschungs- oder Statistikzweck dies erfordert.

(3) Der Verantwortliche darf personenbezogene Daten nur veröffentlichen, wenn die betroffene Person eingewilligt hat oder dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist.

Art. 89 DSGVO: Garantien und Ausnahmen in Bezug auf die Verarbeitung zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken

(1) Die Verarbeitung zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken unterliegt geeigneten Garantien für die Rechte und Freiheiten der betroffenen Person gemäß dieser Verordnung. Mit diesen Garantien wird sichergestellt, dass technische und organisatorische Maßnahmen bestehen, mit denen insbesondere die Achtung des Grundsatzes der Datenminimierung gewährleistet wird. Zu diesen Maßnahmen kann die *Pseudonymisierung* gehören, sofern es möglich ist, diese Zwecke auf diese Weise zu erfüllen. In allen Fällen, in denen diese Zwecke durch die Weiterverarbeitung, bei der die Identifizierung von betroffenen Personen nicht oder nicht mehr möglich ist, erfüllt werden können, werden diese Zwecke auf diese Weise erfüllt.

(2) Werden personenbezogene Daten zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken verarbeitet, können vorbehaltlich der Bedingungen und Garantien gemäß Absatz 1 des vorliegenden Artikels im Unionsrecht oder im Recht der Mitgliedstaaten insoweit Ausnahmen von den Rechten gemäß der Artikel 15, 16, 18 und 21 vorgesehen werden, als diese Rechte voraussichtlich die Verwirklichung der spezifischen Zwecke unmöglich machen oder ernsthaft beeinträchtigen und solche Ausnahmen für die Erfüllung dieser Zwecke notwendig sind.

(3) Werden personenbezogene Daten für im öffentlichen Interesse liegende Archivzwecke verarbeitet, können vorbehaltlich der Bedingungen und Garantien gemäß Absatz 1 des vorliegenden Artikels im Unionsrecht oder im Recht der Mitgliedstaaten insoweit Ausnahmen von den Rechten gemäß der Artikel 15, 16, 18, 19, 20 und 21 vorgesehen werden, als diese Rechte voraussichtlich die Verwirklichung der spezifischen Zwecke unmöglich machen oder ernsthaft beeinträchtigen und solche Ausnahmen für die Erfüllung dieser Zwecke notwendig sind.
(4) Dient die in den Absätzen 2 und 3 genannte Verarbeitung gleichzeitig einem anderen Zweck, gelten die Ausnahmen nur für die Verarbeitung zu den in diesen Absätzen genannten Zwecken.

2.2 Zulässigkeit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nur zulässig, wenn eine Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Die Einwilligung ist regelmäßig schriftlich zu erteilen. Zuvor ist der Betroffene auf den Zweck der Verarbeitung hinzuweisen mit den entsprechenden Hinweisen bzgl. Einschränkung seiner Rechte aufgrund des Wissenschaftsprivilegs. Bereits als Vorfrage für die Zulässigkeit der Datenverarbeitung ist von Bedeutung, ob überhaupt personenbezogene Daten benötigt werden. Gestaltung und Auswahl von Datenverarbeitungsprogrammen haben sich nämlich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Dies kann beispielsweise durch eine vollständige Anonymisierung erreicht werden, die sicherstellt, dass die betroffene Person nicht identifiziert werden kann. Da dies in vielen Fällen nur eingeschränkt möglich ist, ist insbesondere von der Möglichkeit der *Pseudonymisierung* Artikel 4 Absatz 5 (Art. 4 DSGVO 2018) Gebrauch zu machen.

Art. 4 DSGVO Absatz (5): Pseudonymisierung

„Pseudonymisierung bezeichnet die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.“

Im Falle von SQ2050 werden nicht direkt personenbezogene Daten erhoben, jedoch können durch die erhobenen Daten Rückschlüsse auf die Personen gezogen werden. Die im Projekt generierten Daten werden für zwei Beispielquartiere erhoben und sind somit eindeutig den Bewohnern dieser

Quartiere zuzuordnen. Zusätzlich werden einige Datenpunkte, wie beispielsweise Energieverbrauch, Raumtemperatur und Bewohnerverhalten, auf Wohnungsebene erfasst. In Kombination mit Charakteristika der jeweiligen Wohnung lassen sich Rückschlüsse auf einzelne Personen oder Personengruppen ziehen. Dadurch entstehen diverse Anforderungen an die Datenerhebung, -speicherung und -verarbeitung, die im Folgenden beispielhaft beschrieben werden.

Um das Prinzip der Datensparsamkeit einzuhalten, müssen beispielsweise Überlegungen zur notwendigen Granularität der Zeitintervalle, in denen Verbrauchsdaten automatisiert erhoben werden, angestellt werden. Eine feingranulare Erhebung der Daten kann aus Datenschutzgründen durchaus vertretbar sein, wenn die höhere Auflösung eine höhere Prognosegenauigkeit bewirken kann. Weiterhin ist der Grundsatz der Erforderlichkeit zu berücksichtigen. Danach ist die Datenverarbeitung nur zulässig, wenn sie zur Aufgabenerfüllung erforderlich ist.

2.3 Technische und organisatorische Maßnahmen

Die im Rahmen von SQ2050 erhobenen Daten sind in vielerlei Hinsicht von verschiedenen Risiken betroffen, die dazu führen können, dass erhobene Daten unbrauchbar werden, verloren gehen oder manipuliert werden, indem z. B. IT-Systeme versagen, Mechanismen zum Schutz vor unberechtigter Löschung und Veränderung der Daten fehlen sowie eine unzureichende Datenspeicherung vorliegt. Zum Schutz der personenbezogenen Daten sind von den Daten verarbeitenden Stellen die notwendigen *technischen und organisatorischen Maßnahmen* zu treffen, die erforderlich sind, um die Ausführung der Vorschriften des BDSG zu gewährleisten. Artikel 32 der DSGVO (Art. 32 DSGVO 2018) spezifiziert dies genauer:

> Artikel 32 DSGVO Absatz (1):
>
> „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 treffen der Verantwortliche und der Auftragsverarbeiter **geeignete technische und organisatorische Maßnahmen**, um ein dem **Risiko angemessenes Schutzniveau** zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:
>
> a) die **Pseudonymisierung** und **Verschlüsselung** personenbezogener Daten;

b) die Fähigkeit, die **Vertraulichkeit, Integrität, Verfügbarkeit** und **Belastbarkeit** der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

c) die Fähigkeit, die **Verfügbarkeit** der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch **wiederherzustellen**;

d) ein Verfahren zur regelmäßigen **Überprüfung**, **Bewertung** und **Evaluierung** der **Wirksamkeit** der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung."

Ergänzend beschreibt (§ 64 BDSG 2018) einzuhaltende "Gebote", die 14 Kontrollziele, z. B. Zutrittskontrolle, Zugangskontrolle und Zugriffskontrolle vorgeben. Die zu ergreifenden Maßnahmen werden im Gesetz nicht konkret beschrieben, da ihre Eignung vom jeweiligen Anwendungsfall und dem Schutzbedarf der personenbezogenen Daten abhängig ist und die technischen Maßnahmen einem permanenten Wandel unterliegen.

Datenschutzmaßnahmen können in der Planungs- und Konzeptionsphase, im Zuge der Umsetzung sowie beim Betrieb von IT-Systemen und -Verfahren verankert sein. In der DSGVO werden dazu die Konzepte *Privacy by Design* und *Privacy by Default* ausgeführt, die die zwei wesentlichen Elemente zum Schutz personenbezogener Daten und zur Umsetzung der Grundsätze aus Artikel 5 der DSGVO (Art. 5 DSGVO 2018) darstellen.

Der Ansatz von *Privacy by Design* legt den Fokus auf die Einbettung technischer und organisatorischer Maßnahmen in den gesamten Entwicklungsprozess aller zugrundeliegenden Prozesse und verwendeten (IT)Systeme, die bei der zukünftigen Datenverarbeitung Anwendung finden. Dadurch wird sichergestellt, dass Datenschutz nicht nur durch die Einhaltung von Vorschriften gewährleistet wird, sondern bereits bei der Konzeptionierung sämtlicher Organisationsstrukturen, der IT-Infrastruktur und den verwendeten Prozessen berücksichtigt wird. Grundlage hierfür ist Artikel 25 Absatz 1 der DSGVO (Art. 25 DSGVO 2018).

Das Konzept *Privacy by Default* ergänzt das Prinzip des Privacy by Design, indem es vorschreibt, dass die zur Anwendung kommenden Prozesse und technischen Systeme anwenderfreundlich bzgl. Datenschutz zu gestalten sind. Anwendern soll auf einfache Weise einerseits die Möglichkeit gegeben werden, datenschutzfreundlichere Einstellungen der Systeme eigenhändig vorzunehmen und andererseits befähigt werden, die Verarbeitung ihrer personenbezogenen Daten auf einfache Weise zu überwachen sowie einzuschränken bzw. zu erweitern. Grundlage ist Artikel 25 Absatz 2 (Art. 25 DSGVO 2018).

Artikel 25 DSGVO Absatz (1): Privacy by Design

„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 der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung **geeignete technische und organisatorische Maßnahmen** - wie z. B. Pseudonymisierung - trifft, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen."

Artikel 25 DSGVO Absatz (2): Privacy by Default

„Der Verantwortliche trifft **geeignete technische und organisatorische Maßnahmen**, die sicherstellen, dass durch **Voreinstellung** grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten **Verarbeitungszweck erforderlich** ist, verarbeitet werden. Diese Verpflichtung gilt für die **Menge** der erhobenen personenbezogenen Daten, den **Umfang** ihrer Verarbeitung, ihre **Speicherfrist** und ihre **Zugänglichkeit**. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden."

Besonderer Schutzbedarf besteht bei automatisierten Abrufverfahren. Bei diesen Online-Verfahren trägt die empfangende Stelle die Verantwortung für die Zulässigkeit des Abrufs. Im Falle von SQ2050 sind dies beispielsweise Daten, die über die in den Quartieren installierte Smart-Meter-Technik erhoben werden oder automatisiert von den Energieversorgern zur Verfügung gestellt werden.

2.4 Rechte der Betroffenen

Die Betroffenen haben nach dem BDSG Abschnitt 1-5 (Kap. 3 DSGVO 2018) und den landesspezifischen Datenschutzgesetzen insbesondere die folgenden Rechte:

- **Recht auf Auskunft** über die zu ihrer Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen, die

Empfänger oder Kategorien von Empfängern, an die die Daten weitergegeben werden und den Zweck der Speicherung.

- **Recht auf Berichtigung**, wenn unrichtige Daten gespeichert werden.
- **Recht auf Sperrung**, soweit die Richtigkeit der Daten vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt.
- **Recht auf Löschung**, wenn die Speicherung der Daten unzulässig ist oder die Daten nicht mehr benötigt werden. An die Stelle einer Löschung tritt eine Sperrung, soweit Aufbewahrungsfristen entgegenstehen, der Grund zur Annahme besteht, dass die Löschung schutzwürdige Interessen der Betroffenen beeinträchtigen würde oder die Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohen Aufwand möglich ist.
- **Recht auf Widerspruch** gegen die Datenverarbeitung wegen der besonderen persönlichen Situation des Betroffenen, sofern die Datenverarbeitung nicht durch eine Rechtsvorschrift verlangt wird.
- **Recht auf Schadensersatz** wegen einer unzulässigen oder unrichtigen Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten.

Diese Rechte können nicht durch Verträge oder sonstige Rechtsgeschäfte ausgeschlossen oder beschränkt werden. Darüber hinaus kann sich der Betroffene zu Fragen des Datenschutzes auch an den betrieblichen bzw. behördlichen Datenschutzbeauftragten (bDSB) oder die jeweils zuständige Aufsichtsbehörde wenden. Niemand darf benachteiligt oder gemaßregelt werden, weil er sich an den Datenschutzbeauftragten oder die Aufsichtsbehörde gewandt hat. Form- und Fristerfordernisse bestehen nicht.

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

3 Technische und organisatorische Maßnahmen

Im Rahmen des Datenschutzes müssen die rechtlichen Rahmenbedingungen beachtet und geeignete *technische und organisatorische Maßnahmen* getroffen werden, um den Datenschutz sicher zu stellen. Die Maßnahmen teilen sich grundsätzlich in **drei Phasen** auf:

- Planung und Konzeption
- Umsetzung
- Betrieb

3.1 Planung und Konzeption

Bei der Planung und Konzeption aller im Verbund verwendeten IT-Systeme, IT-Verfahren und Prozesse, die zur Verarbeitung personenbezogener Daten eingesetzt werden, sind Maßnahmen zur Umsetzung eines wirksamen Datenschutzes zu unternehmen.

3.1.1 Datenschutzmanagement

Mit Datenschutzmanagement werden die Prozesse bezeichnet, die notwendig sind, um die Umsetzung der gesetzlichen Anforderungen des Datenschutzes bei der Planung, Einrichtung, dem Betrieb und nach Außerbetriebnahme von Verfahren zur Informationsverarbeitung sicherzustellen.

Herzstück des Datenschutzmanagements ist der Datenschutzprozess. Er ist wie der Sicherheitsprozess als zyklischer Prozess ausgelegt, um bei geändertem Umfeld die Einhaltung des geltenden Datenschutzrechts kontinuierlich sicherstellen zu können. Er deckt die Aufgaben in einer Organisation ab, die sich auf strategischer, taktischer oder operativer Ebene ergeben. Der Prozess bedient sich dabei einzelner Maßnahmen, die im Folgenden beschrieben werden.

Initialisierung des Datenschutzprozesses

In diesem Prozessschritt sind Maßnahmen angesiedelt, die eine strategische Zielstellung (Geltungsdauer bis zu fünf Jahren) haben. Sie beinhalten:

- Erarbeitung einer Datenschutz-Richtlinie, in der Regel im Rahmen einer behörden- oder unternehmensweiten Sicherheitsrichtlinie.

- Einrichtung eines Datenschutzmanagements, in der Regel innerhalb des Sicherheitsmanagements. Wichtige Teilaspekte sind die Regelung der Zuständigkeiten, Prozessdefinitionen und Bereitstellung von Ressourcen (Personalkapazitäten).

Normalerweise existieren bei den am Projekt beteiligten Partnern bereits Datenschutz- und Datensicherheitsrichtlinien, die bei Bedarf und auf geeignete Weise an die im Rahmen des Projekts neu hinzukommenden Anforderungen angepasst und um weitere Richtlinien und Regelungen ergänzt werden müssen. Bereits bei der Planung des Projekts sollten diejenigen Personen, die aktuell für den Datenschutz bei den beteiligten Projektpartner zuständig sind, sich um die Anpassung der geltenden Konzepte und Richtlinien kümmern.

Umsetzung der erforderlichen Maßnahmen

Dieser Prozessschritt beinhaltet die Umsetzung der im Datenschutzkonzept festgelegten, bislang noch nicht umgesetzten Maßnahmen (Kapitel 3.2). Die Umsetzung erfolgt im Rahmen eines klassischen Projektmanagements mit einem Projekt- und Arbeitsplan, welcher von den beteiligten Partnern, die mit der Verarbeitung der Daten zukünftig betraut sein werden, zu erstellen und umzusetzen ist. Dies hat zu erfolgen, sobald die Verantwortlichkeiten und Rollen der Projektpartner für den laufenden Betrieb festgelegt sind. Jeder Partner hat sodann je nach Umfang seiner Aufgaben und Rollen und den dazugehörigen Verantwortlichkeiten die in diesem Konzept festgelegten Maßnahmen umzusetzen und weitere Maßnahmen zu bestimmen, die zum Zeitpunkt der Erstellung des Datenschutzkonzeptes noch nicht festgelegt werden können.

Aufrechterhaltung des Datenschutzes im laufenden Betrieb

Die Aufgabe dieses Teilprozesses ist es, auf Änderungen und Störungen im laufenden Betrieb der Verfahren zu reagieren, in denen personenbezogener Daten verarbeitet werden. Dies sind vor allem:

- Änderungen im Datenschutzrecht
- Änderungen in den (IT-)Verfahren
- Störungen in den operativen Betriebsabläufen, die als Sicherheitsvorfall zu klassifizieren sind
- Technischer Fortschritt und reduzierter Aufwand für bisher nicht realisierte Maßnahmen.

Zu diesem Zweck wird begleitend zum Sicherheitsprozess eine Reihe von Sub-Prozessen benötigt, die Änderungen und Störungen aus Datenschutz-

sicht eigenständig bearbeiten bzw. lösen. Die Ergebnisse können gegebenenfalls auch Strukturänderung im Datenschutzmanagement oder Aktualisierungen des Datenschutzkonzeptes zur Folge haben.

Management von Sicherheitsvorfällen

Das Management von Sicherheitsvorfällen bei IT-Verfahren im laufenden Betrieb muss auch gegebenenfalls die Vorfälle und ihre Folgen unter dem Gesichtspunkt des geltenden Datenschutzrechtes behandeln. Dies geschieht zweckmäßigerweise in Zusammenarbeit mit dem IT-Sicherheitsbeauftragten des jeweiligen verantwortlichen Partners, der das Sicherheitsvorfall-Team leitet. Aufgaben des begleitenden Datenschutzmanagements können hier sein:

- Priorisierung von technischen und organisatorischen Maßnahmen zur Problemanalyse und Problemlösung bzw. Beweissicherung unter Datenschutzgesichtspunkten
- Behandlung juristischer Aspekte unter dem Gesichtspunkt des Datenschutzrechtes.

Unter dem Gesichtspunkt der Prozessintegration ist es sinnvoll, dass der Sicherheitsprozess das entsprechende Datenschutzmanagement auslöst bzw. den entsprechenden Sub-Prozess aufruft. Im zukünftigen Betrieb kann dies beispielsweise bedeuten, dass bei Sicherheitsvorfällen, die die in den Quartieren installierte Technik, die bei den beteiligten Partnern installierte Hardware und Software zur Datenverarbeitung bzw. zugehörige Verfahren und Prozesse betreffen, in denen personenbezogene Daten verarbeitet werden, der Datenschutzbeauftragte des verantwortlichen Partners automatisch Mitglied des Sicherheitsvorfall-Teams wird. Er kann so in die Informationen und Prozessabläufe optimal eingebunden werden. Unter diesem Management ist auch eine Beschreibung zu verstehen, wo bzw. von wem im Unternehmen Datenschutzvorfälle gemanagt werden.

Management der Lebenszyklen von IT-Verfahren unter Datenschutzgesichtspunkten

Beim Management der Lebenszyklen von IT-Produkten und -Verfahren kommt ein Lebenszyklusmodell zur Anwendung, das sich am allgemeinen Lebenszyklusmodell der BSI-Standards und der IT-Grundschutz-Kataloge orientiert.

Darüber hinaus sollte bei der Planung und Konzeption von neuen IT-Verfahren geprüft werden, ob Privacy Enhancing Technologies (PETs) eingesetzt werden können. PETs unterstützen technisch die Umsetzung von Daten-

schutzgrundsätzen wie Datensparsamkeit, Zweckbindung oder das Transparenzgebot. Beispiele für PETs sind Protokolle wie P3P (Platform for Privacy Preferences) und Verfahren zur Anonymisierung und Pseudonymisierung von Daten beim Netzwerktransfer, der Datenhaltung in Datenbanken oder dem Data Mining (Privacy Preserving Data Mining, PPDM). Aber auch Wiedervorlagefunktionen in Programmen, die die Einhaltung von Löschfristen bei der Speicherung von personenbezogenen Daten unterstützen, zählen dazu.

Management von Änderungen im Datenschutzrecht

Änderungen im Datenschutzrecht sind zu verfolgen und hinsichtlich ihrer Auswirkungen auf die Verfahren, in denen personenbezogene Daten verarbeitet werden, zu beurteilen. Dieser Sub-Prozess lässt sich auch in das behörden- oder unternehmensweite Monitoring von Änderungen in relevanter Gesetzgebung integrieren.

Technologie-Monitoring

Das Technologie-Monitoring verfolgt gemeinsam mit dem Sicherheits-Management den "Stand der Technik" bezogen auf Informationssicherheit und Datenschutz. Unter Maßgabe der einschlägigen Datenschutzgesetzgebung und deren Anwendung gibt dieser Sub-Prozess Impulse für die Weiterentwicklung von Datenschutz- und Sicherheitskonzept.

Monitoring und Management von Änderungen in den IT-Grundschutz-Katalogen

Beim allgemeinen Monitoring sind auch Aktualisierungen der BSI-Standards und der IT-Grundschutz-Kataloge, insbesondere des Datenschutzbausteins zu berücksichtigen. Neben Impulsen für die Weiterentwicklung von Datenschutz- und Sicherheitskonzept sind auch die Schnittstellen zu Sicherheitsmanagement zu überprüfen und gegebenenfalls anzupassen.

3.1.2 Regelung von Verantwortlichkeiten

Für alle wesentlichen Aufgaben und Prozesse, die in Verbindung mit der Verarbeitung der erhobenen Daten stehen, sollten die Verantwortlichkeiten nachvollziehbar geregelt sein. Die sicherheitsrelevanten Aufgaben aller internen und externen Mitarbeiter der am Projekt beteiligten Partner (Stadt,

Stadtwerke, Baugesellschaften, Forschungsorganisationen etc.) müssen nachvollziehbar festgelegt sein. Sie müssen mit den Sicherheitszielen der beteiligten Institutionen abgestimmt sein. Zu den Bereichen, die geregelt werden sollten, gehören beispielsweise:

- explizite Zuweisung der Verantwortlichkeiten und Befugnisse an Rollen bzw. Organisationseinheiten bei allen sicherheitsrelevanten Aufgaben (Dabei ist sicherzustellen, dass alle Rollen konkreten Personen zugeordnet sind),
- Vertraulichkeitsvereinbarungen,
- Festlegung von Verhaltensregeln und Informationspflichten bei sicherheitsrelevanten Aktionen und bei Sicherheitsvorfällen,
- Klassifikation von Informationen entsprechend ihres Schutzbedarfs.

Die Regelungen für Informationssicherheit sollten mit denen für Datenschutz und Geheimschutz in geeigneter Weise zusammengeführt werden, damit sie von den Mitarbeitern leichter adaptiert und besser wahrgenommen werden können. Wichtig ist auch, dass alle Regelungen zusammengenommen widerspruchsfrei sind. Übergreifende Regelungen zur Informationssicherheit müssen als ein Aspekt der Informationsverarbeitung verbindlich festgelegt werden.

Als Grundlage für die Regelung der Verantwortlichkeiten gelten die bestehenden Datenschutz- und Datensicherheitsvereinbarungen der beteiligten Partner. Diese sind bzgl. neu hinzukommender Anforderungen und Regeln aufgrund den zukünftig im Rahmen des Projektes zu verarbeitenden Daten zu erweitern und anzupassen. Dazu gehört es, Regelungen über die Themen

- Datensicherung,
- Datenarchivierung,
- Datenübertragung,
- Dokumentation von IT-Verfahren, Software, IT-Konfiguration,
- Zugriffsberechtigungen,
- Wartungs- und Reparaturarbeiten,
- Datenschutz,
- Schutz gegen Schadsoftware,
- Vorgehensweise bei der Verletzung von Sicherheitsrichtlinien

zu treffen und ggf. die vorliegenden Konzepte der am Projekt beteiligten Partner zu ergänzen.

Die Datensicherung betrifft alle Vorgänge, die zur Absicherung von Datenmissbrauch zu unternehmen sind, wie z.B. die Absicherung gegen den unberechtigten Zugriff, die unberechtigte Veränderung und unberechtigte Einsicht von Daten durch nicht befugte Dritte mittels geeigneter Sicherheitssoftware. Ebenso gehört dazu die Absicherung gegen Viren und Trojaner, die die IT der Projektpartner und die Sicherheit der Daten gefährden können.

Dazu ist es notwendig alle zur IT gehörenden Komponenten, die zur Verarbeitung von Daten genutzt werden, entsprechend zu dokumentieren, um sie für die verantwortlichen Mitarbeiter transparent zu machen. Für die Archivierung der im Projekt manuell und mittels Smart Meter Technik erhobenen Daten gilt es ebenfalls Regelungen bzgl. Verantwortlichkeiten festzulegen. Es gilt festzulegen, wer mit der Verarbeitung digital und manuell erhobener Daten beauftragt werden darf und welche Personen in welchem Umfang Zugriff auf die erhobenen Daten haben, um diese zu Speichern und ggf. auch auf andere Speichermedien zu übertragen (digital wie manuell über einen Kopiervorhang zwischen Hardwarekomponenten). Auch für die Wartung der in den Quartieren verbauten Geräte (Smart Meter Technik) gilt es die verantwortlichen Mitarbeiter festzulegen, da hier die Möglichkeit besteht die Geräte in einer Art und Weise zu verändern, so dass Daten fehlerhaft erhoben oder unberechtigt eingesehen werden können.

Die in Kraft gesetzten Regelungen sind den betroffenen Mitarbeitern (Mitarbeiter, die mit der Verarbeitung von Daten betraut sind) in geeigneter Weise bekannt zu geben. Es empfiehlt sich, die Bekanntgabe zu dokumentieren. Darüber hinaus sind sämtliche Regelungen in der aktuellen Form an einer Stelle vorzuhalten und bei berechtigtem Interesse zugänglich zu machen. Die getroffenen Regelungen sind regelmäßig zu aktualisieren, um Missverständnisse, ungeklärte Zuständigkeiten und Widersprüche zu vermeiden und gegebenenfalls aufzulösen. Alle Regelungen sollten deshalb auch ein Erstellungsdatum oder eine Versionsnummer enthalten.

3.1.3 Prüfung rechtlicher Rahmenbedingungen und Vorabkontrolle bei der Verarbeitung personenbezogener Daten

Im Rahmen der Prüfung der rechtlichen Rahmenbedingungen als Voraussetzung der Datenverarbeitung müssen folgende Aspekte betrachtet werden:

- Prüfung, ob personenbezogene Daten verarbeitet werden
- Zulässigkeit der Datenverarbeitung
- Erforderlichkeit der Datenverarbeitung
- Verwendung der Daten hinsichtlich der Zweckbindung
- Durchführung einer Vorabkontrolle

Bei der Betrachtung dieser Aspekte sollte wegen eventuell schwieriger Rechtsmaterie, insbesondere zu Datenschutzfragen, auf juristische Unterstützung zurückgegriffen werden. Hier ist zu prüfen, ob die auf Quartiersebene erhobenen Daten personenbezogen sind. Dies wäre dann der Fall, wenn nur aufgrund der Daten auf einzelne Personen eines Quartiers rückgeschlossen werden kann. Die Zulässigkeit der Datenverarbeitung ist im Falle von SQ2050 gegeben, da ohne die Erhebung von Daten der angestrebte Zweck (Prognose von Energieverbrauch, Energieeinsparungsempfehlungen) nicht erfüllbar wäre.

Zulässigkeit der Datenverarbeitung

Für die Verarbeitung und Nutzung personenbezogener Daten gilt als allgemeiner Grundsatz ein sogenanntes Verbot mit Erlaubnisvorbehalt (z. B. § 4 Abs. 1 BDSG). Die Prüfung der Zulässigkeit der Datenverarbeitung sollte im Regelfall in Zusammenarbeit mit den fachlich zuständigen Stellen erfolgen.

Vor der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten ist zu prüfen, ob

- dies durch die Datenschutzgesetze oder eine andere Rechtsvorschrift ausdrücklich erlaubt
  oder angeordnet ist oder
- der Betroffene gemäß § 4 BDSG oder entsprechender landes- oder spezialgesetzlicher Regelungen eingewilligt hat.

Bei der Speicherung, Veränderung und Übermittlung personenbezogener Daten durch nicht-öffentliche Stellen ist zu prüfen, ob dies

- im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen erfolgt oder
- zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zur Annahme besteht, dass das schutzwürdige Interesse an dem Ausschluss der Verarbeitung oder Nutzung überwiegt (im Sinne von §§ 28 ff. BDSG).

Dazu müssen alle Bewohner, die sich entscheiden in eines der entsprechenden Quartiere einzuziehen, zuvor eine Datenschutzerklärung unterzeichnen, die die Bewohner darüber aufklärt, welche Daten, in welchem Umfang und zu welchem Zweck verarbeitet werden und das die Erhebung, die Speicherung sowie die Verarbeitung seiner Daten zur Zielerreichung notwendig ist.

Prüfung der Erforderlichkeit

Nach dem Prinzip der Erforderlichkeit gilt der Grundsatz, dass personenbezogene Daten nur erhoben werden dürfen, wenn sie für die Aufgabenerfüllung erforderlich sind. Das ist der Fall, wenn ohne ihre Kenntnis die Durchführung der betreffenden Aufgaben (Energieverbrauchsprognosen, Betrieb der Quartiers-App und des Grid Optimizers) unmöglich oder wesentlich erschwert wäre. Im hier vorliegenden Fall ist die Erhebung von Quartiers- und Bewohnerdaten essentiell, da diese zur Analyse von Zusammenhängen zwischen Energieverbrauch und spezifischem Verhalten benötigt werden, um auf deren Basis Empfehlungen zur Energieeinsparung an die Bewohner automatisiert weitergeben zu können. Dabei muss jedoch sichergestellt werden, dass die einzelnen Partner nur auf diejenigen Daten zugreifen dürfen,

die für die Erfüllung ihrer Aufgaben erforderlich sind. Mitarbeiter der Landeshauptstadt Stuttgart und der Stadt Überlingen, der Baugenossenschaft Überlingen und der Stuttgarter Wohnungs- und Städtebaugesellschaft sowie der Stadtwerke Stuttgart und der Stadtwerke am See dürfen somit nur mit der Verarbeitung derjenigen Daten betraut werden, die auch durch die jeweilige Organisation erhoben wurden. Falls die Daten zentral an einem Ort gespeichert und verarbeitet werden, sind nur die Mitarbeiter der entsprechenden Einrichtung mit der Datenverarbeitung zu betrauen. Da zum Zeitpunkt der Erstellung dieses Konzeptes nicht feststeht, wo die erhobenen Daten zu den Quartieren bzw. deren Bewohnern gespeichert bzw. verarbeitet werden, können aktuell keine bestimmten Mitarbeiter mit der Aufgabe der Datenverarbeitung betraut werden. Sobald die Rollen bzgl. Datenschutz für den laufenden Betrieb von den Verantwortlichen Personen der beteiligten Partner festgelegt wurden, sind die Verantwortlichkeiten bzgl. Datenverarbeitung hier näher festzulegen. Schwierigkeiten bereitet dies hinsichtlich der Systemverwalter. Sie haben in den marktüblichen Systemen beliebigen Zugriff auf alle Daten. Auch sie müssen in bestimmtem Umfang im Zugriff beschränkt werden. Geeignete Maßnahmen hierfür sind:

- Verschlüsselung der Daten,
- Zugriffsbeschränkungen,
- abgestufte Berechtigungskonzepte,
- Menüführung,
- Aufteilung der Systemadministratorfunktionen auf verschiedene Rollen sowie
- die sichere Protokollierung der Aktivitäten des Systemverwalters.

Bei der Gestaltung von Technik sind solche Verfahren zu wählen, bei denen möglichst wenig personenbezogene Daten verarbeitet werden. Es gilt das Gebot der Datenvermeidung bzw. Datensparsamkeit. Soweit möglich, sind Verfahren anonym zu gestalten oder Pseudonyme zu verwenden. Bei der Erhebung der Quartiersdaten sowie der zugehörigen Energieverbräuche oder Daten zu den Bewohnern eines Quartiers, sind die Daten so zu verschlüsseln, dass die Mitarbeiter keinen direkten Bezug zu den Bewohnern des jeweiligen Quartiers herstellen können.

Prüfung der Verwendung von Daten hinsichtlich der Zweckbindung

Vor der Speicherung, Veränderung und Nutzung personenbezogener Daten ist zu prüfen, ob dies für die Zwecke erfolgt, für die die Daten erhoben worden sind bzw., falls keine Erhebung voranging, es für die Zwecke erfolgt, für die sie gespeichert worden sind. Von diesem Zweckbindungsgrundsatz gibt es eine Reihe, zum Teil weit reichender gesetzlicher Ausnahmen (siehe z. B. § 14 BDSG).

Vorabkontrolle

Im Rahmen der Vorabkontrolle ist vor dem erstmaligen Einsatz automatisierter Verfahren zur Bearbeitung personenbezogener Daten zu prüfen, welche Gefahren hierdurch für das informationelle Selbstbestimmungsrecht erwachsen können. Eine Vorabkontrolle ist nicht durchzuführen, wenn eine gesetzliche Verpflichtung oder eine Einwilligung des Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient. Automatisierte Verfahren dürfen nur dann eingesetzt werden, wenn sichergestellt ist, dass keine Gefahren für das informationelle Selbstbestimmungsrecht bestehen.

3.1.4 Festlegung von technisch-organisatorischen Maßnahmen entsprechend dem Stand der Technik bei der Verarbeitung personenbezogener Daten

Welche Maßnahmen notwendig sind, damit das Recht auf informationelle Selbstbestimmung gewährleistet ist und die personenbezogenen Daten vor Missbrauch, Fehlern und Unglücksfällen möglichst sicher sind, hängt nicht nur von der Art der Daten und der Aufgabe ab, für die sie verwendet werden sollen, sondern ebenso von den organisatorischen Bedingungen, den räumlichen Verhältnissen, der personellen Situation und anderen Rahmenbedingungen. In zukünftigen Versionen dieses Konzepts sollen dazu konkrete Maßnahmen zur Sicherstellung von Datenschutz und -sicherheit definiert werden. Nach aktuellem Arbeits- und Informationsstand im Projekt lassen sich hierzu noch keine genauen Aussagen machen.

Nach §9 BDSG müssen die Maßnahmen geeignet sein,

- Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (**Zutrittskontrolle**),
- zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (**Zugangskontrolle**),
- zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (**Zugriffskontrolle**),
- zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (**Weitergabekontrolle**),

- zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (**Eingabekontrolle**),
- zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (**Auftragskontrolle**),
- zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (**Verfügbarkeitskontrolle**),
- zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Der Aufwand für die notwendigen Maßnahmen sollte in einem angemessenen Verhältnis zum angestrebten Schutzzweck stehen. Je schwerer die den Betroffenen drohende Rechtsverletzung und je größer das Risiko eines Schadenseintritts ist, umso höher ist der angemessene Aufwand. Ein Ermessen besteht zwar bei der Auswahl der einzelnen Maßnahmen, nicht aber bei der Festlegung des Schutzniveaus.

Als notwendig erkannte Maßnahmen sind auch dann zu treffen, wenn sie die Entwicklung und den Einsatz einer IT-Anwendung erschweren. Ist dies mit den vorgesehenen Maßnahmen nicht zu gewährleisten, muss entweder ein höherer Aufwand in Kauf genommen werden oder eine andere, mit weniger Aufwand verbundene Verfahrensgestaltung in Betracht gezogen werden. Diese Maßnahmen sind entsprechend dem aktuellen Stand der Technik fortzuschreiben.

Eine Auswahl technisch-organisatorischer Maßnahmen, die zum Einsatz kommen können sind

- das physikalische Löschen von Daten,
- die kryptographische Verschlüsselung,
- interne IT- und Datenschutz-Regelungen sowie
- Protokollierung und Dokumentation von Verfahren, um die Nachvollziehbarkeit zu gewährleisten.

3.2 Umsetzung

3.2.1 Organisatorische Verfahren zur Sicherstellung der Rechte der Betroffenen bei der Verarbeitung personenbezogener Daten

Es sind technisch-organisatorische Verfahren zu entwickeln, um die Durchsetzung der Rechte der Betroffenen auf Auskunft, Berichtigung, Sperrung, Löschung sowie Einsicht in Dateien- bzw. Verfahrensverzeichnisse (soweit solche Verzeichnisse vorgeschrieben sind) sicherzustellen. Diese Verfahren sollen so beschaffen sein, dass die Rechte der Betroffenen schnell und zweckmäßig umgesetzt werden können.

Mögliche Maßnahmen sind:

- Ein Verfahren zur Verarbeitung personenbezogener Daten enthält ein Auswerteprogramm
  oder einen Menüpunkt, mit dessen Hilfe ein vollständiger Ausdruck der gespeicherten Daten des Betroffenen erzeugt wird.
- Ein Verfahrensverzeichnis wird mit Hilfe einer Datenbank so automatisiert, dass über bestimmte Stichworte ein sehr einfacher Zugriff auf den umfangreichen Datenbestand möglich ist und damit alle Querbezüge erkannt werden können.
- Mittels einer Menüfunktion per Knopfdruck ist es den Betroffenen möglich eine automatisch erzeugte Mailvorlage zu erstellen, die die Verantwortlichen über Fehler in den personenbezogenen Daten unterrichtet und den Auftrag erteilt die fehlerhaften Daten zu berichtigen.
- Das Auswerteprogramm zur Erstellung des Datenauszuges enthält auch die Möglichkeit alle vorhandenen Daten mittels einer einfachen Zustimmung per Knopfdruck zu löschen.

3.2.2 Führung von Verfahrensverzeichnissen und Erfüllung der Meldepflicht

Neben den zentralen Datenverarbeitungsanlagen sind bei dezentraler Datenverarbeitung alle eingesetzten IT-Systeme zu erfassen. Es muss jederzeit auf ein aktuelles Verzeichnis der eingesetzten Hardware (Monitoring- und Steuergerät), Software (Quartiers-App, Grid Optimizer) und Verfahren (Analyseverfahren) sowie der erfassten personenbezogenen Daten zugegriffen werden können. In einigen Datenschutzvorschriften gibt es konkrete Vorgaben für die Ausgestaltung dieser Verzeichnisse. Verfahren automatisierter Verarbeitungen zur Erhebung, Verarbeitung oder Nutzung personenbezogener Daten sind von der verantwortlichen Stelle in einer Übersicht (Verfahrensverzeichnis) zu führen. Die Übersicht enthält grundsätzlich die Angaben nach §§ 4d und 4e BDSG und wird nach § 4g Absatz 2 BDSG in den meisten Fällen vom bDSB geführt.

3.2.3 Datenschutzrechtliche Freigabe

Software und IT-Verfahren sind mit systematisch entwickelten Fall-Konstellationen (Testdaten, keine personenbezogenen Echtdaten) nach einem Testplan, aus dem das gewünschte Ergebnis hervorgeht, zu überprüfen. Massentests können, wenn erforderlich, nach Zustimmung und Vorgaben der fachlich dafür zuständigen Stelle mit anonymisierten Originaldaten durchgeführt werden. Die Zustimmung der fachlich zuständigen Stelle zur Anonymisierung von Originaldaten und alle Testergebnisse sind revisionssicher zu dokumentieren. Im Folgenden werden Maßnahmen zum Testen von Software erläutert. Dazu wird der Prozess des Testens in die Abschnitte Vorbereitung, Durchführung und Auswertung unterteilt.

Testvorbereitung

- Festlegung der Testmethoden für die Einzeltests (Testarten, -verfahren und -werkzeuge)
- Generierung von Testdaten und Testfällen
- Aufbau der benötigten Testumgebung

Festlegung der Testmethoden für die Einzeltests (Testarten, -verfahren und -werkzeuge)

Methoden zur Durchführung von Tests sind z. B. statistische Analyse, Simulation, Korrektheitsbeweis, symbolische Programmausführung, Review, Inspektion, Versagensanalyse. Hierbei muss beachtet werden, dass einige dieser Testmethoden nur bei Vorliegen des Quellcodes durchführbar sind. In der Vorbereitungsphase muss die geeignete Testmethode ausgewählt und festgelegt werden.

Es muss geklärt werden, welche Verfahren und Werkzeuge zum Testen von Programmen und zum Prüfen von Dokumenten eingesetzt werden. Typische Verfahren zum Testen von Programmen sind z. B. Black-Box-Tests, White-Box-Tests oder Penetrationstests. Dokumente können z. B. durch informelle Prüfungen, Reviews oder anhand von Checklisten kontrolliert werden.

Ein Black-Box-Test ist ein Funktionalitätstest ohne Kenntnis der internen Programmabläufe, bei dem z. B. das Programm mit allen Datenarten für alle Testfälle mit Fehlerbehandlung und Plausibilitätskontrollen durchlaufen wird. Bei einem White-Box-Test handelt es sich um einen Funktionalitätstests unter Offenlegung der internen Programmabläufe, z. B. durch Quellcode-Überprüfung oder Tracing. White-Box-Tests gehen in der Regel über den IT-Grundschutz hinaus und können für Standardsoftware in der Regel nicht durchgeführt werden, da der Quellcode vom Hersteller nicht offengelegt wird. Bei Funktionalitätstests soll der Nachweis erbracht werden soll, dass der Testinhalt der Spezifikation entspricht. Durch Penetrationstests soll festgestellt werden, ob bekannte oder vermutete Schwachstellen im praktischen Betrieb ausgenutzt werden können, beispielsweise durch Manipulationsversuche an den Sicherheitsmechanismen oder durch Umgehung von Sicherheitsmechanismen durch Manipulationen auf Betriebssystemebene.

Weiterhin ist die Art und Weise der Ergebnissicherung und -auswertung festzuschreiben, insbesondere im Hinblick auf die Wiederholbarkeit von Prüfungen. Es muss geklärt werden, welche Daten während und nach der Prüfung festzuhalten sind.

Generierung von Testdaten und Testfällen

Die Vorbereitung von Tests umfasst auch die Generierung von Testdaten. Methode und Vorgehensweise sind zuvor festzulegen und zu beschreiben. Für jeden einzelnen Testinhalt muss eine dem Testaufwand angemessene Anzahl von Testfällen generiert werden. Jede der folgenden Kategorien ist dabei zu berücksichtigen:

- **Standardfälle** sind Fälle, mit denen die korrekte Verarbeitung der definierten Funktionalitäten überprüft werden soll. Die eingehenden Daten nennt man Normalwerte oder Grenzwerte. **Normalwerte** sind Daten innerhalb, **Grenzwerte** sind Eckdaten des jeweils gültigen Eingabebereichs.
- **Fehlerfälle** sind Fälle, in denen versucht wird, mögliche Fehlermeldungen des Programms zu provozieren. Diejenigen Eingabewerte, auf die das Programm mit vorgegebenen Fehlermeldungen reagieren soll, nennt man **Falschwerte**.
- **Ausnahmefälle** sind Fälle, bei denen das Programm ausnahmsweise anders reagieren muss als bei Standardfällen. Es muss daher überprüft werden, ob das Programm diese Fälle als solche erkennt und korrekt bearbeitet.

Testdaten sollten aus allen Daten bestehen, die im späteren Realbetrieb von der Quartiers-App verwendet werden, um auf Basis der Daten den Bewohnern der Quartiere Empfehlungen zur Energieeinsparung über die installierten Monitoring- und Steuerungseinheiten zu geben. Dabei sollten Daten generiert werden, die zum einen Normwerte abbilden und auf deren Basis die Quartiers-App und der Grid Optimizer zuvor erarbeitete Empfehlungen geben. Jedoch sollten auch Daten generiert werden, die zu unsinnigen Empfehlungen oder am besten zu einer Fehlermeldung des Systems führen. Genauso sollten Daten generiert werden, die Ausnahmefälle abbilden, um zu prüfen, ob auch unkonventionelle Empfehlungen durch das System vorgeschlagen werden. Ist die Generierung von Testdaten zu aufwendig oder schwierig, können auch anonymisierte Echtdaten für den Test eingesetzt werden. Aus Gründen des Vertraulichkeitsschutzes müssen Echtdaten unbedingt zuverlässig anonymisiert werden. Zu beachten bleibt, dass die anonymisierten Echtdaten u. U. nicht alle Grenzwerte und Ausnahmefälle abdecken, so dass diese gesondert erzeugt werden müssen.

Über die Testdaten hinaus sollten auch alle Arten möglicher Benutzerfehler betrachtet werden. Problematisch sind insbesondere alle Benutzerreaktionen, die im Programmablauf nicht vorgesehen und dementsprechend nicht korrekt abgewiesen werden.

Aufbau der benötigten Testumgebung

Die im Testplan beschriebene Testumgebung muss aufgebaut und die zu testenden Produkte (Quartiers-App, Grid Optimizer, Smart Meter, Monito-

ring- und Steuergeräte) dort installiert werden. Die eingesetzten Komponenten sind zu identifizieren und deren Konfiguration ist zu beschreiben. Treten bei der Installation des Produktes Abweichungen von der beschriebenen Konfiguration auf, so ist dies zu dokumentieren.

Testdurchführung

- Eingangsprüfungen
- Funktionale Tests
- Tests weiterer funktionaler Eigenschaften
- Sicherheitsspezifische Tests
- Pilotanwendung

Die Durchführung der Tests muss anhand des Testplans erfolgen. Jede Aktion sowie die Testergebnisse müssen ausreichend dokumentiert und bewertet werden (z.B. mittels Punktesystem). Insbesondere wenn Fehler auftreten, sind diese derart zu dokumentieren, dass sie reproduziert werden können (Fehlerart, zugehörige Systemkonfiguration, Auswirkungen, betroffene Systemkomponenten etc.). Die für den späteren Produktionsbetrieb geeigneten Betriebsparameter müssen ermittelt und für die spätere Erstellung einer Installationsanweisung in Form eines Handbuchs festgehalten werden. Zeigt sich bei Bearbeitung einzelner Testinhalte, dass eine oder mehrere Anforderungen des Anforderungskataloges nicht konkret genug waren, sind diese gegebenenfalls zu konkretisieren.

Eingangsprüfungen

Vor allen anderen Tests sind zunächst die folgenden grundlegenden Aspekte zu testen, da ein Misserfolg bei diesen Eingangsprüfungen zu direkten Aktionen oder dem Testabbruch führt:

- Die Computer-Virenfreiheit des Produktes (Quartiers-App, Grid Optimizer, Smart Meter, Monitoring- und Steuergerät) ist durch ein aktuelles Virensuchprogramm zu überprüfen.
- In einem Installationstest muss festgestellt werden, ob das Produkt für den späteren Einsatzzweck einfach, vollständig und nachvollziehbar zu installieren ist. Ebenfalls muss überprüft werden, wie das Produkt vollständig deinstalliert wird.
- Die Lauffähigkeit des Produktes ist in der geplanten Einsatzumgebung (Quartier, Wohnung) zu überprüfen; dies beinhaltet insbesondere eine Überprüfung der Bildschirmaufbereitung, der Menüführung, der Netzfähigkeit, etc.
- Die Vollständigkeit des Produktes ist zu überprüfen, z. B. durch einen Vergleich mit dem Bestandsverzeichnis, der Produktbeschreibung oder ähnlichem.

- Es sollten Kurztests von Funktionen des Programms durchgeführt werden, die nicht explizit in den Anforderungen erwähnt wurden, im Hinblick auf Funktion, Plausibilität, Fehlerfreiheit, etc.

Funktionale Tests

Die funktionalen Anforderungen, die im Anforderungskatalog an das Produkt gestellt wurden, sind auf folgende Aspekte zu untersuchen.

- *Existenz der Funktion* durch Aufruf im Programm und Auswertung der Programmdokumentationen.
- Fehlerfreiheit bzw. Korrektheit der Funktion
  Um die Fehlerfreiheit bzw. Korrektheit der Funktion sicherzustellen, sind je nach Prüftiefe bei der Untersuchung unterschiedliche Testverfahren wie Black-Box-Tests, White-Box-Tests oder simulierter Produktionsbetrieb anzuwenden. Die in der Vorbereitungsphase erstellten Testdaten und Testfälle werden im Funktionalitätstest eingesetzt. Bei den Funktionalitätstests ist es notwendig, die Testergebnisse mit den vorgegebenen Anforderungen zu vergleichen. Außerdem ist zu überprüfen, wie das Programm bei fehlerhaften Eingabeparametern oder fehlerhafter Bedienung reagiert. Die Funktion ist auch mit den Grenzwerten der Intervalle von Eingabeparametern sowie mit Ausnahmefällen zu testen. Diese müssen entsprechend erkannt und korrekt behandelt werden.
- Eignung der Funktion
  Die Eignung einer Funktion zeichnet sich dadurch aus, dass die Funktion
  - tatsächlich die Aufgabe im geforderten Umfang und effizient erfüllt und
  - sich leicht in die üblichen Arbeitsabläufe integrieren lässt.
- Widerspruchsfreiheit
  Die Widerspruchsfreiheit der einzelnen Funktionen ist zu überprüfen und zwar jeweils zwischen Anforderungskatalog, Dokumentation und Programm. Eventuelle Widersprüche sind zu dokumentieren. Abweichungen zwischen Dokumentation und Programm sind so festzuhalten, dass sie bei einem späteren Einsatz des Produktes in den Ergänzungen zur Dokumentation aufgenommen werden können.

Tests weiterer funktionaler Eigenschaften

Die im Anforderungskatalog neben den funktionalen und den sicherheitsspezifischen Anforderungen spezifizierten weiteren funktionalen Eigenschaften sind ebenfalls zu überprüfen:

- Performance (Grid Optimizer, Quartiers-App, Monitoring- und Steuergerät)
  Das Laufzeitverhalten sollte für alle geplanten Konfigurationen des

Produktes ermittelt werden. Um die Performance ausreichend zu testen, sind in der Regel Tests, in denen der Produktionsbetrieb simuliert wird oder auch Pilotanwendung bei ausgewählten Anwendern sinnvoll. Es muss festgestellt werden, ob die gestellten Performanceanforderungen erfüllt sind.

- Zuverlässigkeit (Grid Optimizer, Quartiers-App, Monitoring- und Steuergerät)
  Das Verhalten bei zufälligen oder mutwillig herbeigeführten Systemabstürzen ("Crash-Test") ist zu analysieren und es ist festzustellen, welche Schäden dabei entstehen. Es ist festzuhalten, ob nach Systemabstürzen ein ordnungsgemäßer und korrekter Wiederanlauf des Produktes möglich ist. Es ist ebenfalls zu überprüfen, ob ein direkter Zugriff auf Datenbestände unabhängig von der regulären Programmfunktion erfolgen kann. In vielen Fällen kann ein solcher Zugriff zu Datenverlusten führen und sollte dann vom Produkt verhindert werden. Ebenfalls sollte festgehalten werden, ob das Programm Möglichkeiten unterstützt, "kritische Aktionen" (z. B. Löschen, Formatieren) rückgängig zu machen.
- Benutzerfreundlichkeit (Quartiers-App, Monitoring- und Steuergerät)
  Ob das Produkt benutzerfreundlich ist, ist in besonderem Maße vom subjektiven Empfinden der Testperson abhängig. Jedoch können bei der Beurteilung folgende Aspekte Anhaltspunkte liefern:
  - Technik der Menüoberflächen (Pull-Down-Menüs, Scrolling, Drag & Drop, etc.),
  - Design der Menüoberflächen (z. B. Einheitlichkeit, Verständlichkeit, Menüführung),
  - Fehlermeldungen,
  - problemloses Ansprechen von Schnittstellen (Batchbetrieb, Kommunikation, etc.),
  - Lesbarkeit der Benutzerdokumentation,
  - Hilfefunktionen.

  Die Analyse der Benutzerfreundlichkeit muss mögliche Betriebsarten des Produktes beschreiben, einschließlich des Betriebes nach Bedien- oder Betriebsfehlern, und ihre Konsequenzen und Folgerungen für die Aufrechterhaltung eines sicheren Betriebes.
- Wartbarkeit (Monitoring- und Steuergerät, Quartiers-App, Smart Meter)
  Der personelle und finanzielle Aufwand für die Wartung und Pflege des Produktes sollte während des Testens ermittelt werden. Dieser kann z. B. anhand von Referenzen wie anderen Referenzinstallationen oder Tests in Fachzeitschriften oder anhand des während des Testens ermittelten Installationsaufwandes geschätzt werden. Hierfür muss dokumentiert werden, wie viele manuelle Eingriffe während der Installation notwendig waren, um die angestrebte Konfiguration zu erreichen. Sind bereits Erfahrungen mit Vorgängerversionen des getesteten Produktes gesammelt worden, sollte hinterfragt werden, wie aufwendig deren Wartung war. Es sollte nachgefragt werden, inwieweit Support durch den Hersteller oder Vertreiber angeboten wird und zu welchen Konditionen. Wird vom Hersteller oder Vertreiber eine Hotline angeboten, sollte auch deren Erreichbarkeit und Güte betrachtet werden.

- Dokumentation (Monitoring- und Steuergerät, Quartiers-App, Grid Optimizer)
  Die vorliegende Dokumentation muss daraufhin überprüft werden, ob sie vollständig, korrekt und widerspruchsfrei ist. Darüber hinaus sollte sie verständlich, eindeutig, fehlerfrei und übersichtlich sein. Es muss weiterhin kontrolliert werden, ob sie für eine sichere Verwendung und Konfiguration ausreicht. Alle sicherheitsspezifischen Funktionen müssen beschrieben sein.

Darüber hinaus sind als weitere Punkte des Anforderungskatalogs zu testen:

- Kompatibilitätsanforderungen
- Interoperabilität
- Konformität zu Standards
- Einhaltung von internen Regelungen und gesetzlichen Vorschriften
- Softwarequalität

Sicherheitsspezifische Tests

Wurden sicherheitsspezifische Anforderungen an das Produkt gestellt, so sind zusätzlich zu den vorgenannten Untersuchungen auch folgende Aspekte zu untersuchen:

- Wirksamkeit und Korrektheit der Sicherheitsfunktionen,
- Stärke der Sicherheitsmechanismen und
- Unumgänglichkeit und Zwangsläufigkeit der Sicherheitsmechanismen.

Als Grundlage für eine Sicherheitsuntersuchung könnte beispielsweise das Handbuch für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEM) herangezogen werden, in dem viele der nachfolgend aufgezeigten Vorgehensweisen beschrieben sind. Die weiteren Ausführungen dienen zur Orientierung.

Zu Beginn muss durch funktionale Tests zunächst nachgewiesen werden, dass das Produkt die erforderlichen Sicherheitsfunktionen bereitstellt. Anschließend ist zu überprüfen, ob alle erforderlichen Sicherheitsmechanismen im Anforderungskatalog genannt wurden, ggf. ist dieser zu ergänzen.

Um die Mindeststärke der Mechanismen zu bestätigen oder zu verwerfen sind **Penetrationstests** durchzuführen. Penetrationstests sind nach allen anderen Tests durchzuführen, da sich aus diesen Tests Hinweise auf potentielle Schwachstellen ergeben können. Durch Penetrationstests kann das Testobjekt (Monitoring- und Steuergerät) oder die Testumgebung beschädigt oder beeinträchtigt werden. Damit solche Schäden keine Auswirkungen haben, sollten vor der Durchführung von Penetrationstests Datensicherungen gemacht werden. Penetrationstests können durch Verwendung von Sicherheitskonfigurations- und Protokollierungstools unterstützt werden. Diese

Tools untersuchen eine Systemkonfiguration und suchen nach gemeinsamen Schwachstellen wie etwa allgemein lesbaren Dateien und fehlenden Passwörtern.

Mit Penetrationstests soll das Produkt auf Konstruktionsschwachstellen untersucht werden, indem dieselben Methoden angewandt werden, die auch ein potentieller Angreifer zur Ausnutzung von Schwachstellen benutzen würde, wie z. B.

- Ändern der vordefinierten Befehlsabfolge,
- Ausführen einer zusätzlichen Funktion,
- Direktes oder indirektes Lesen, Schreiben oder Modifizieren interner Daten,
- Ausführen von Daten, deren Ausführung nicht vorgesehen ist,
- Verwenden einer Funktion in einem unerwarteten Kontext oder für einen unerwarteten Zweck,
- Aktivieren der Fehlerüberbrückung,
- Nutzen der Verzögerung zwischen dem Zeitpunkt der Überprüfung und dem Zeitpunkt der Verwendung,
- Unterbrechen der Abfolge durch Interrupts, oder
- Erzeugen einer unerwarteten Eingabe für eine Funktion.

Die Mechanismenstärken werden anhand der Begriffe Fachkenntnisse, Gelegenheiten und Betriebsmittel definiert, in der ITSEM werden diese näher erläutert.

Beispielsweise können zur Bestimmung der Mechanismenstärke folgende Regeln angewandt werden:

- Kann der Mechanismus innerhalb von Minuten von einem Laien allein überwunden werden, dann kann er **nicht einmal als niedrig** eingestuft werden.
- Kann ein erfolgreicher Angriff von jedem bis auf einen Laien innerhalb von Minuten durchgeführt werden, dann ist der Mechanismus als **niedrig** einzustufen.
- Wenn für einen erfolgreichen Angriff ein Experte benötigt wird, der mit der vorhandenen Ausstattung Tage braucht, dann ist der Mechanismus als **mittel** einzustufen.
- Kann der Mechanismus nur von einem Experten mit Sonderausstattung überwunden werden, der dafür Monate braucht und eine geheime Absprache mit einem Systemverwalter treffen muss, dann ist er als **hoch** einzustufen.

Es muss sichergestellt werden, dass die durchgeführten Tests alle sicherheitsspezifischen Funktionen umfassen. Wichtig ist zu beachten, dass durch Testen immer nur Fehler oder Abweichungen von den Spezifikationen festgestellt werden können, niemals jedoch die Abwesenheit von Fehlern. Typische Untersuchungsaspekte sind die folgenden:

Passwortschutz:

- Gibt es vom Hersteller voreingestellte Passwörter? Typische Beispiele für solche Passwörter sind der Produktname, der Herstellername, "SUPERVISOR", "ADMINISTRATOR", "USER", "GUEST".
- Welche Datei ändert sich, wenn ein Passwort geändert wurde? Kann diese Datei durch eine alte Version aus einer Datensicherung ersetzt werden, um alte Passwörter zu aktivieren? Werden die Passwörter verschlüsselt gespeichert oder sind sie im Klartext auslesbar? Ist es möglich, in dieser Datei Änderungen vorzunehmen, um neue Passwörter zu aktivieren?
- Wird der Zugang tatsächlich nach mehreren fehlerhaften Passworteingaben gesperrt?
- Werden in Zeitschriften oder Mailboxen Programme angeboten, die die Passwörter des untersuchten Produkts ermitteln können? Für einige Standardapplikationen sind solche Programme erhältlich.
- Wenn Dateien mit Passwörtern geschützt werden, kann durch einen Vergleich einer Datei vor und nach der Passwortänderung die Stelle ermittelt werden, an der das Passwort gespeichert wird. Ist es möglich, an dieser Stelle Änderungen oder alte Werte einzugeben, um bekannte Passwörter zu aktivieren? Werden die Passwörter verschlüsselt gespeichert? Wie ist die Stelle belegt, wenn der Passwortschutz deaktiviert ist?
- Kann die Passwort-Prüfroutine unterbrochen werden? Gibt es Tastenkombinationen, mit denen die Passworteingabe umgangen werden kann?

Zugriffsrechte:

- In welchen Dateien werden Zugriffsrechte gespeichert und wie werden sie geschützt?
- Können Zugriffsrechte von Unberechtigten geändert werden?
- Können Dateien mit alten Zugriffsrechten zurückgespielt werden und welche Rechte benötigt man dazu?
- Können die Rechte des Administrators so eingeschränkt werden, dass er keinen Zugriff auf die Nutz- oder Protokolldaten erhält?

Datensicherung:

- Können erstellte Datensicherungen problemlos rekonstruiert werden?
- Können Datensicherungen durch ein Passwort geschützt werden? Wenn ja, können die oben dargestellten Untersuchungsansätze für Passwörter eingesetzt werden.

Verschlüsselung:

- Bietet das Produkt an, Dateien oder Datensicherungen zu verschlüsseln?
- Werden mehrere verschiedene Verschlüsselungsalgorithmen angeboten? Hierbei ist im allgemeinen folgende Faustregel zu beachten:

"Je schneller ein in Software realisierter Verschlüsselungsalgorithmus ist, um so unsicherer ist er."

- Wo werden die zur Ver- oder Entschlüsselung genutzten Schlüssel gespeichert?
  Bei einer lokalen Speicherung ist zu untersuchen, ob diese Schlüssel passwortgeschützt oder mit einem weiteren Schlüssel überschlüsselt geschützt werden. Bei einem **Passwortschutz** sind die obigen Punkte zu berücksichtigen. Bei einer Überschlüsselung ist zu betrachten, wie der zugehörige Schlüssel geschützt wird. Dazu können folgende Punkte betrachtet werden: Welche Datei ändert sich, wenn ein Schlüssel geändert wurde? Durch den Vergleich dieser Datei vor und nach der Schlüsseländerung kann die Stelle ermittelt werden, an der dieser Schlüssel gespeichert wird. Ist es möglich, an dieser Stelle Änderungen vorzunehmen, um neue Schlüssel zu aktivieren, die dann vom Anwender genutzt werden, ohne dass dieser die Kompromittierung bemerkt?
- Gibt es vom Hersteller voreingestellte Schlüssel, die vor der erstmaligen Benutzung des Programms geändert werden müssen?
- Was passiert, wenn bei der Entschlüsselung ein falscher Schlüssel eingegeben wird?
- Wird nach der Verschlüsselung einer Datei die unverschlüsselte Variante gelöscht? Wenn ja, wird sie zuverlässig überschrieben? Wird vor der Löschung überprüft, ob die Verschlüsselung erfolgreich war?

Protokollierung:

- Wird der Zugriff auf Protokolldaten für Unbefugte verwehrt?
- Werden die zu protokollierenden Aktivitäten lückenlos aufgezeichnet?
- Hat der Administrator die Möglichkeit aufgrund seiner privilegierten Rechte, sich unberechtigt und unbemerkt Zugriff auf Protokolldaten zu verschaffen oder kann er die Protokollierung unbemerkt deaktivieren?
- Wie reagiert das Programm, wenn der Protokollierungsspeicher überläuft?

Darüber hinaus muss festgestellt werden, ob durch das neue Produkt Sicherheitseigenschaften an anderer Stelle unterlaufen werden, z.B. ob das zu testende Produkt (Monitoring- und Steuergerät, Quartiers-App, Grid Optimizer) eine Schnittstelle zu anderen gekoppelten (IT-)Systemen besitzt, zuvor aber keine solchen Schnittstellen existierten.

Pilotanwendung:

Nach Abschluss aller anderen Tests kann noch eine Pilotanwendung, also ein Einsatz unter Echtbedingungen, für notwendig gehalten werden. Erfolgt der Test in der Produktionsumgebung (Quartier) mit Echtdaten, muss vorab durch eine ausreichende Anzahl von Tests die korrekte und fehlerfreie Funktionsweise aller Komponenten (Monitoring- und Steuergerät, Smart Metern) und der zugehörigen Programme (Quartiers-App, Grid Optimizer) bestätigt worden sein, um die Verfügbarkeit und Integrität der Produktionsumgebung

nicht zu gefährden. Dabei kann das Produkt beispielsweise bei ausgewählten Benutzern (Bewohnern in Bestandsgebäuden) installiert werden, die es dann für einen gewissen Zeitraum im echten Produktionsbetrieb einsetzen.

Testauswertung

Anhand festgelegter Entscheidungskriterien sind die Testergebnisse zu bewerten, alle Ergebnisse zusammenzuführen und mit der Testdokumentation der Beschaffungsstelle bzw. Testverantwortlichen vorzulegen. Anhand der Testergebnisse sollte ein abschließendes Urteil für die zu beschaffenden Produkt gefällt werden. Hat kein Produkt den Test bestanden, muss überlegt werden, ob eine neue Marktsichtung vorgenommen werden soll, ob die gestellten Anforderungen zu hoch waren und geändert werden müssen oder ob von einer Beschaffung zu diesem Zeitpunkt abgesehen werden muss.

Weiter muss geregelt sein, wie IT-Verfahren abgenommen, freigegeben, eingespielt bzw. benutzt werden dürfen. Der Einsatz von IT zur Aufgabenbewältigung setzt voraus, dass die maschinelle Datenverarbeitung soweit wie möglich fehlerfrei arbeitet, da die Kontrolle der Einzelergebnisse in den meisten Fällen nicht mehr zu leisten ist. Im Zuge eines Software-Abnahme-Verfahrens wird deshalb überprüft, ob die betrachtete Software fehlerfrei arbeitet, das heißt, ob die Software die erforderliche Funktionalität zuverlässig bereitstellt und ob sie darüber hinaus keine unerwünschten Nebeneffekte hat. Mit der anschließenden Freigabe der Software durch die fachlich zuständige Stelle wird die Erlaubnis erteilt, die Software zu nutzen. Gleichzeitig übernimmt diese Stelle damit auch die Verantwortung für das IT-Verfahren, dass durch die Software realisiert wird.

Bei der Software-Abnahme unterscheidet man sinnvollerweise zwischen Software, die selbst oder im Auftrag entwickelt wurde, und Standardsoftware, die nur für den speziellen Einsatzzweck angepasst wird.

Abnahme von selbst- oder im Auftrag entwickelter Software

Bevor der Auftrag zur Software-Entwicklung intern oder extern vergeben wird, muss die Anforderungsdefinition für die Software erstellt sein, aus der dann das Grob- und Feinkonzept für die Realisierung entwickelt wird. Anhand dieser Dokumente erstellt die fachlich zuständige Stelle, nicht die für die Software-Entwicklung zuständige Stelle, im allgemeinen einen Abnahmeplan.

Üblicherweise werden hierzu Testfälle und die erwarteten Ergebnisse für die Software erarbeitet. Anhand dieser Testfälle wird die Software getestet und

der Abgleich zwischen berechnetem und erwartetem Ergebnis wird als Indiz für die Korrektheit der Software benutzt.

Zur Entwicklung der Testfälle und zur Durchführung der Tests ist folgendes zu beachten:

- die Testfälle werden von der fachlich zuständigen Stelle entwickelt,
- für Testfälle werden keine Daten des Wirkbetriebs benutzt,
- Testdaten, insbesondere wenn sie durch Kopieren der Wirkdaten erstellt werden, dürfen keine vertraulichen Informationen beinhalten; personenbezogene Daten sind zu anonymisieren oder zu simulieren,
- die Durchführung der Tests darf keine Auswirkungen auf den Wirkbetrieb haben; nach Möglichkeit sollte ein logisch oder physikalisch isolierter Testrechner benutzt werden.

Eine Abnahme ist zu verweigern, wenn:

- schwerwiegende Fehler in der Software festgestellt werden,
- Testfälle auftreten, in denen die erwarteten Ergebnisse nicht mit den berechneten übereinstimmen und
- Benutzerhandbücher oder Bedienungsanleitungen nicht vorhanden oder von nicht ausreichender Qualität sind und
- die Software, unter anderem der Quellcode und die Abläufe, nicht oder nicht ausreichend dokumentiert ist.

Die Ergebnisse der Abnahme sind schriftlich festzuhalten. Die Dokumentation des Abnahmeergebnisses sollte umfassen:

- Bezeichnung und Versionsnummer der Software und gegebenenfalls des IT-Verfahrens,
- Beschreibung der Testumgebung,
- Testfälle und Testergebnisse und
- Abnahmeerklärung.

Abnahme von Standardsoftware

Wird Standardsoftware beschafft, so sollte auch diese einer Abnahme und einer Freigabe unterzogen werden. In der Abnahme sollte überprüft werden, ob

- die Software frei von Computer-Viren ist,
- die Software kompatibel zu den anderen eingesetzten Produkten ist,
- die Software in der angestrebten Betriebsumgebung lauffähig ist und welche Parameter zu setzen sind,
- die Software komplett einschließlich der erforderlichen Handbücher ausgeliefert wurde und
- die geforderte Funktionalität erfüllt wird.

Dazu gehört Software zur Aufbereitung und Auswertung der Daten als auch die Software, die den Grid Optimizer steuert und die Quartiers-App sowie die Software auf den installierten Smart-Metern und der Monitoring- und Steuerungseinheit, die in den Quartieren angebracht ist.

Freigabe-Verfahren

Ist die Abnahme der Software erfolgt, muss die Software für die Nutzung freigegeben werden. Dazu ist zunächst festzulegen, wer berechtigt ist, Software freizugeben. Die Freigabe der Software ist schriftlich festzulegen und geeignet zu hinterlegen.

Die Freigabeerklärung sollte umfassen:

- Bezeichnung und Versionsnummer der Software und gegebenenfalls des IT-Verfahrens,
- Bestätigung, dass die Abnahme ordnungsgemäß vorgenommen wurde,
- Einschränkungen für die Nutzung (Parametereinstellung, Benutzerkreis,...),
- Freigabedatum, ab wann die Software eingesetzt werden darf und
- die eigentliche Freigabeerklärung.

Falls IT-technisch möglich, muss verhindert werden, dass Software nach der Freigabe unbemerkt verändert oder manipuliert werden kann, beispielsweise durch geeignete Verfahren zum Integritätsschutz. Andernfalls müssen geeignete organisatorische Regelungen festgelegt werden, um Änderungen an der Software zu verhindern bzw. zeitnah festzustellen.

Auch nach intensiven Abnahmetests kann es vorkommen, dass im laufenden Einsatz Fehler in der Software festgestellt werden. Für diesen Fall ist festzulegen, wie in einem solchen Fehlerfall verfahren werden soll (Ansprechpartner, Fehlerbeseitigungsablauf, Beteiligung der fachlich zuständigen Stelle, Wiederholung der Abnahme und Freigabe, Versionskontrolle).

Die Freigabe von IT-Verfahren mit der Verarbeitung personenbezogener Daten setzt eine Prüfung auch aus datenschutzrechtlicher Sicht voraus.

3.2.4 Meldung und Regelung von Abrufverfahren bei der Verarbeitung personenbezogener Daten

Den automatisierten Abrufverfahren (Smart-Meter-Technik) kommt unter dem Aspekt des Datenschutzes und der Datensicherung besondere Bedeutung zu, weil die abrufende Stelle (Energieversorger, Netzbetreiber, Wohnungsbaugesellschaft etc.) je nach Einrichtung eines solchen Anschlusses

ohne Einzelentscheidung der zuständigen Stelle über den gesamten Bestand oder wesentliche Teile der von der übermittelnden Stelle bereitgehaltenen personenbezogenen Daten verfügen kann. Deshalb sehen die entsprechenden gesetzlichen Regelungen (z. B. § 10 BDSG) den technischen und organisatorischen Datenschutz zwingend bereits als Teil der Planung von Abrufverfahren vor.

Automatisierte Abrufverfahren werden in den Datenschutzgesetzen als eine Phase der Datenverarbeitung definiert, bei der gespeicherte oder durch Datenverarbeitung gewonnene personenbezogene Daten an einen Dritten in der Weise bekannt gegeben werden, dass die Daten durch die datenverarbeitende Stelle zum Abruf bereitgestellt werden und der Abruf durchgeführt wird.

Die Verantwortung für die Zulässigkeit des einzelnen Abrufs trägt der Empfänger.

Für die Einrichtung eines automatisierten Abrufverfahrens sind die besonderen Zulässigkeitsvoraussetzungen in den einschlägigen Gesetzen dargestellt. Zur Kontrollierbarkeit der Zulässigkeit sind die wesentlichen Details des Abrufverfahrens schriftlich festzulegen. Zu beachten ist, dass die Unterrichtung des Bundes- bzw. Landesbeauftragten für den Datenschutz über die Einrichtung eines Abrufverfahrens in einigen Datenschutzgesetzen gefordert ist.

Allgemeine Aspekte:

- Anlass und Zweck (Monitoring, Datenauswertung, Anreizsetzung) sowie beteiligte Stellen (Stadtwerke, Stadt Stuttgart, Überlingen, Fraunhofer IBP etc.) am Abrufverfahren sind festzulegen.
- Abrufberechtigungen sind festzulegen und zu kontrollieren.
- Art und Umfang der bereitgehaltenen Daten sind festzulegen.
- Sperr- und Löschfristen für Daten sind zu definieren.
- Es ist festzulegen, in welchen Fällen die speichernde Stelle (Stadtwerke, Stadt Stuttgart, Stadt Überlingen etc.) von der abrufenden Stelle (IBP, FIT, App-Betreiber etc.) zu informieren ist.

Maßnahmen gegen unbefugten Abruf:

- Nach einer festgelegten Anzahl von Fehlversuchen ist die Berechtigung zu sperren.
- Passwörter müssen in regelmäßigen Abständen gewechselt werden. Soweit möglich, ist dies durch die entsprechenden Programme zu erzwingen.
- Der Abruf besonderer Arten personenbezogener Daten muss durch ein höheres Schutzniveau gesichert werden (Besitz und Wissen).
- Zur Überprüfung der Protokolldateien sollten programmgesteuerte Prüfungsverfahren eingesetzt werden.
- Art und Umfang der Protokollierung müssen festgelegt werden.

- Es sollten zufallsgesteuerte Stichprobenkontrollen oder eine Dauerprotokollierung durchgeführt werden.
- Es ist festzulegen, an welcher Stelle die Protokollierungen durchgeführt werden, ob bei der abrufenden Stelle, bei der speichernden Stelle, oder an beiden Stellen.
- Die Protokollierung muss so konzipiert sein, dass nachträglich festgestellt werden kann, aufgrund wessen Abrufberechtigung Daten abgerufen wurden.
- Die Gründe des Abrufs müssen protokolliert werden.
- Beim Abruf von Daten sollte protokolliert werden, über welchen Anschluss und welche Endgeräte die Übertragung stattfindet.

Netzanbindung:

Bei der Vernetzung von IT-Systemen (Grid Optimizer, Monitoring- und Steuergerät, Server mit Analysealgorithmus etc.) ist zu überprüfen, wie der Netzanschluss der Endsysteme realisiert ist. Bei Wählanschlüssen ist beispielsweise zu überprüfen, welche Sicherheitsmaßnahmen vorgesehen sind, bei virtuellen Festverbindungen, ob geschlossene Benutzergruppen eingerichtet worden sind. In lokalen Netzen sollten geschlossene Benutzergruppen so eingerichtet werden, dass sie jeweils nur geschlossene Organisationseinheiten umfassen.

3.2.5 Regelung der Auftragsdatenverarbeitung bei der Verarbeitung personenbezogener Daten

Werden personenbezogene Daten im Auftrag verarbeitet, bleibt der Auftraggeber (Stadtwerke, Stadt Stuttgart, Stadt Überlingen) für die Einhaltung der Gesetze und Vorschriften über den Datenschutz verantwortlich. Er hat den Auftragnehmer (Stadtwerke, Stadt Stuttgart, Stadt Überlingen) sorgfältig auszuwählen. Der Auftrag ist im Rahmen der gesetzlichen Vorgaben schriftlich zu erteilen und etwaige Unterauftragsverhältnisse sind festzulegen (§ 11 BDSG).

Je nachdem, wie schutzbedürftig die personenbezogenen Daten sind, die im Auftrag verarbeitet werden sollen, sind die Anforderungen an den Vertrag mit dem Auftragnehmer zu stellen: Je schutzbedürftiger, umso enger und präziser der Auftrag. Auftragnehmer müssen sicherstellen, dass Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden. Unterauftragsverhältnisse unterliegen der Zustimmung des Auftraggebers.

Wenn der Auftragnehmer keine öffentliche Stelle ist, sind die mit der Verarbeitung personenbezogener Daten beschäftigten Personen bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Der Auftraggeber und gegebenenfalls der zuständige Datenschutzbeauftragte haben ein jederzeitiges Kontrollrecht.

3.3 Betrieb

3.3.1 Datenschutzaspekte bei der Protokollierung

Unter Protokollierung beim Betrieb von IT -Systemen ist im datenschutzrechtlichen Sinn die Erstellung von manuellen oder automatisierten Aufzeichnungen zu verstehen, aus denen sich die Fragen beantworten lassen: "Wer hat wann mit welchen Mitteln was veranlasst bzw. worauf zugegriffen?" Außerdem müssen sich Systemzustände ableiten lassen: "Wer hatte von wann bis wann welche Zugriffsrechte?"

Art und Umfang von Protokollierungen hängen vom allgemeinen Datenschutzrecht und auch von bereichsspezifischen Regelungen ab.

Die Protokollierung der Administrationsaktivitäten entspricht einer Systemüberwachung, während die Protokollierung der Benutzeraktivitäten im Wesentlichen der Verfahrensüberwachung dient. Dementsprechend finden sich die Anforderungen an die Art und den Umfang der systemorientierten Protokollierung überwiegend im allgemeinen Datenschutzrecht, während die verfahrensorientierte Protokollierung oft durch bereichsspezifische Regelungen definiert wird.

Mindestanforderungen an die Protokollierung

Bei der *Administration von IT-Systemen* zur Verarbeitung (Speicherung, Auswertung) der erhobenen Daten (Energieverbräuche, Bewohnerdaten, Quartiersdaten) sind die folgenden Aktivitäten vollständig zu protokollieren:

- **Systemgenerierung und Modifikation von Systemparametern**
  Da auf dieser Ebene in der Regel keine systemgesteuerten Protokolle erzeugt werden, bedarf es entsprechender detaillierter manueller Aufzeichnungen, die mit der Systemdokumentation korrespondieren sollten.
- **Einrichten von Benutzern**
  Wem von wann bis wann durch wen das Recht eingeräumt worden ist, das betreffende IT-System zu benutzen, ist vollständig zu protokollieren. Für diese Protokolle sollten längerfristige Aufbewahrungszeiträume vorgesehen werden, da sie Grundlage praktisch jeder Revisionsmaßnahme sind.
- **Erstellung von Rechteprofilen**
  Im Rahmen der Protokollierung der Benutzerverwaltung kommt es insbesondere auch darauf an aufzuzeichnen, wer die Anweisung zur Einrichtung bestimmter Benutzerrechte erteilt hat.
- **Einspielen und Änderung von Anwendungssoftware**
  Die Protokolle repräsentieren das Ergebnis der Programm- und Verfahrensfreigaben.
- **Änderungen an der Dateiorganisation**
  Im Hinblick auf die vielfältigen Manipulationsmöglichkeiten, die sich

bereits bei Benutzung der "Standard-Dateiverwaltungssysteme" ergeben, kommt einer vollständigen Protokollierung eine besondere Bedeutung zu (siehe z. B. Datenbankmanagement).

- **Durchführung von Datensicherungsmaßnahmen**
  Da derartige Maßnahmen (Backup, Restore) mit der Anfertigung von Kopien bzw. dem Überschreiben von Datenbeständen verbunden sind und häufig in "Ausnahmesituationen" durchgeführt werden, besteht eine erhöhte Notwendigkeit zur Protokollierung.
- **Sonstiger Aufruf von Administrations-Tools**
  Die Benutzung aller Administrations-Tools ist zu protokollieren, um feststellen zu können, ob Unbefugte sich Systemadministrator-Rechte erschlichen haben.
- **Versuche unbefugten Einloggens und Überschreitung von Befugnissen**
  Geht man von einer wirksamen Authentisierungsprozedur und sachgerechten Befugniszuweisungen aus, kommt der vollständigen Protokollierung aller "auffälligen Abnormalitäten" beim Einloggen und der Benutzung von Hard- und Software-Komponenten eine zentrale Bedeutung zu. Benutzer in diesem Sinne ist auch der Systemadministrator.

Maßnahmen zur Erstellung von Rechteprofilen:

Es muss eine Dokumentation der am IT-System zugelassenen Benutzer, angelegten Benutzergruppen und Rechteprofile erfolgen, die in die Verarbeitung der erhobenen Daten eingebunden sind. Dabei gibt es verschiedene Dokumentationsmöglichkeiten wie beispielsweise über

- vorgegebene Administrationsdateien des Systems,
- individuelle Dateien, die vom zuständigen Administrator verwaltet werden,
- in Papierform.

Es sollte eine geeignete Form ausgewählt werden, möglichst einheitlich für die gesamte Institution.

Dokumentiert werden sollten insbesondere folgende Angaben zur Rechtevergabe an Benutzer und Benutzergruppen:

<u>Zugelassene Benutzer:</u>

- zugeordnetes Rechteprofil (gegebenenfalls Abweichungen vom verwendeten Standard-Rechteprofil)
- Begründung für die Wahl des Rechteprofils (und gegebenenfalls der Abweichungen)
- Zuordnung des Benutzers zu einer Organisationeinheit, Raum- und Telefonnummer
- Zeitpunkt und Grund der Einrichtung
- Befristung der Einrichtung

Zugelassene Gruppen:

- zugehörige Benutzer
- Zeitpunkt und Grund der Einrichtung
- Befristung der Einrichtung

Die Dokumentation der zugelassenen Benutzer und Rechteprofile sollte regelmäßig (mindestens alle 6 Monate) daraufhin überprüft werden, ob sie den tatsächlichen Stand der Rechtevergabe widerspiegelt und ob die Rechtevergabe noch den Sicherheitsanforderungen und den aktuellen Aufgaben der Benutzer entspricht. Die vollständige Dokumentation ist Voraussetzung für Kontrollen der vergebenen Benutzerrechte. Die Dokumentation muss so gespeichert beziehungsweise aufbewahrt werden, dass sie vor unbefugtem Zugriff geschützt ist und so, dass auch bei einem größeren Sicherheitsvorfall oder IT-Ausfall darauf zugegriffen werden kann. Falls die Dokumentation in elektronischer Form erfolgt, muss sie in das Datensicherungsverfahren einbezogen werden.

Bei der *Verarbeitung von personenbezogenen Daten* (Bewohnerdaten bzw. -verhalten, Quartiersdaten) sind folgende Benutzeraktivitäten in Abhängigkeit von der Sensibilität der Verfahren bzw. Daten vollständig bzw. selektiv zu protokollieren:

- **Eingabe von Daten**
  Die so genannte Eingabekontrolle erfolgt grundsätzlich verfahrensorientiert (z. B. Protokollierung in Akten, soweit vorhanden, Protokollierung direkt im Datenbestand, sofern keine Akten geführt werden). Auch wenn man davon ausgeht, dass Befugnisüberschreitungen anderweitig protokolliert werden, sollte eine vollständige Protokollierung von Dateneingaben (Eingabe erhobener Bewohner- und Quartiersdaten) als Regelfall angesehen werden.
- **Datenübermittlungen**
  Nur soweit nicht gesetzlich eine vollständige Protokollierung vorgeschrieben ist, kann eine selektive Protokollierung als ausreichend angesehen werden.
- **Benutzung von automatisierten Abrufverfahren**
  In der Regel dürfte eine vollständige Protokollierung der Abrufe und der Gründe der Abrufe (Vorgang, Aktenzeichen etc.) erforderlich sein, um unbefugte Kenntnisnahme im Rahmen der grundsätzlich eingeräumten Zugriffsrechte aufdecken zu können.
- **Löschung von Daten**
  Die Durchführung der Löschung ist zu protokollieren, falls Bewohner eines Quartiers ausziehen.
- **Aufruf von Programmen**
  Dies kann erforderlich sein bei besonders "sensiblen" Programmen, die z. B. nur zu bestimmten Zeiten oder Anlässen benutzt werden dürfen. Deshalb ist in diesen Fällen eine vollständige Protokollierung angezeigt. Die Protokollierung dient auch der Entlastung der befugten Benutzer (Nachweis des ausschließlich befugten Aufrufs der Programme).

Zweckbindung bei der Nutzung von Protokolldaten

Protokolldaten unterliegen aufgrund der nahezu übereinstimmenden Regelungen im Datenschutzrecht des Bundes und der Länder einer besonderen engen Zweckbindung. Sie dürfen nur zu den Zwecken genutzt werden, die Anlass für ihre Speicherung waren. Dies sind in der Regel die in einem Sicherheitskonzept festgelegten allgemeinen Kontrollen, die in den meisten Datenschutzgesetzen geforderte Überwachung der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme, mit denen personenbezogene Daten verarbeitet werden und die Kontrollen durch interne oder externe Datenschutzbeauftragte.

Aufbewahrungsdauer

Soweit nicht bereichsspezifische Regelungen etwas anderes vorsehen, richtet sich die Aufbewahrungsdauer der Protokolle nach den allgemeinen Löschungsregeln der Datenschutzgesetze. Protokolldaten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind. Gibt es keinen zwingenden Grund für das weitere Vorhalten von Protokolldateien, besteht eine Löschungspflicht.

Als Anhaltspunkte können dienen:

- die Wahrscheinlichkeit, dass Unregelmäßigkeiten (noch) offenbar werden können und
- die Möglichkeit, die Gründe von Unregelmäßigkeiten anhand der Protokolle und anderer Unterlagen aufdecken zu können.

Erfahrungsgemäß sollte eine Frist von einem Jahr nicht überschritten werden.

Soweit Protokolle zum Zwecke gezielter Kontrollen angefertigt werden, kommen kürzere Speicherungsfristen in Betracht. In der Regel reicht eine Aufbewahrung bis zur tatsächlichen Kontrolle aus. Auch hier sind die bereichsspezifischen Vorschriften zu beachten.

Maßnahmen zur Protokollierung:

Hierzu sei auf den Baustein zur Protokollierung (B.522) des BSI (Bundesamt für Sicherheit in der Informationstechnik) und speziell auf das dafür vorgesehene Maßnahmenbündel zur Protokollierung von IT-Systemen (M2.500). Dieser Baustein betrachtet alle spezifischen Gefährdungen und Maßnahmen, die in einem Informationsverbund (Stadt, Stadtwerke, Energieversorger) unabhängig von den eingesetzten Betriebssystemen für eine angemes-

sene Protokollierung und Überwachung relevant sind. Der Aufwand zur Erstellung und Umsetzung eines solchen Prozesses ist nicht gering. Daher sollte dieser Baustein vor allem bei größeren Informationsverbünden umgesetzt werden.

3.3.2 Dokumentation der datenschutzrechtlichen Zulässigkeit

Bevor Software oder Hardware für die Verarbeitung von personenbezogenen Daten eingesetzt werden, sollten sie, bezogen auf den vorgesehenen Einsatz, auf die datenschutzrechtliche Zulässigkeit geprüft werden. Hier wird es je nach IT-System (z. B. nicht vernetzter PC, zentrales Rechenzentrum, Monitoring- und Steuereinheit, Smart-Meter) sehr unterschiedliche Anforderungen geben. Das Prüfungsergebnis sollte dokumentiert werden. Für Datenschutzkontrollen sind derartige Dokumentationen besonders wichtig.

Der betriebliche bzw. behördliche Beauftragte für den Datenschutz (bDSB) ist nach § 4g Abs. 1 BDSG über Vorhaben der automatisierten Verarbeitung personenbezogener Daten rechtzeitig zu unterrichten. Er hat die ordnungsgemäße Anwendung (vorhandener und neuer) Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet sollen, zu überwachen. Aus diesem Grunde empfiehlt es sich, den bDSB von Anfang an, d.h. im Rahmen der ersten Planungen, mit einzubeziehen. Nur so können bereits in der Planungsphase datenschutzrechtliche Fehler vermieden werden, deren Behebung zu einem späteren Zeitpunkt unter Umständen zeit- und kostenintensiv sein könnten.

3.3.3 Aufrechterhaltung des Datenschutzes im Betrieb

Abgesehen von der Bestellung eines betrieblichen bzw. behördlichen Datenschutzbeauftragten (bDSB) ist die Einrichtung einer internen IT-Revision und Datenschutzkontrolle eine wichtige Maßnahme im Rahmen der durch die Datenschutzgesetze vorgeschriebenen Organisationskontrolle. Sie hilft dabei, vor Ort und zeitnah die Sicherheit der Datenverarbeitung und die Einhaltung der datenschutzrechtlichen Anforderungen zu gewährleisten.

Die IT-Revision überprüft die Ordnungsmäßigkeit der Datenverarbeitung durch Kontrolle der Umsetzung des IT-Sicherheitskonzeptes. Dazu gehören insbesondere eine Kontrolle der Dokumentation der Verfahren, der vorgeschriebenen Verfahrensanwendung und der gesamten Sicherheitsmaßnahmen.

Die interne Datenschutzkontrolle, die meist dem Datenschutzbeauftragten obliegt, überprüft hingegen die Einhaltung der aus den Datenschutzgesetzen herrührenden Anforderungen.

Dazu gehören:

- die Kontrolle der Verfahren auf Einhaltung der Rechtsgrundlage und der Zweckbestimmung,
- die Sicherstellung der Rechte des Betroffenen auf Auskunft, Berichtigung, Sperrung, Löschung und Schadensersatz,
- die Unterrichtung über bzw. die Verpflichtung der Mitarbeiter auf den Datenschutz,
- das Führen von Datei- bzw. Verfahrensübersichten und Geräteverzeichnissen und
- die Kontrolle der aus den gesetzlichen Vorschriften abgeleiteten technisch-organisatorischen Maßnahmen zur Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle und "getrennte Verarbeitung gemäß der Zweckbestimmung".

IT-Revision und Datenschutzkontrolle arbeiten sinnvollerweise zusammen und ergänzen sich. Durch zeitnahe Überprüfung der Protokolldaten helfen sie z. B. mit, einen möglichen Missbrauch schnell aufzudecken und die Aufbewahrungszeit und den Umfang der Protokolldaten so gering wie möglich zu halten. Sie können die Leitung der datenverarbeitenden Stelle bei der Neukonzeption und der Fortentwicklung von Verfahren beraten und dienen als kompetente Ansprechpartner bei Kontrollbesuchen der Aufsichtsbehörden oder des Bundes- und der Landesbeauftragten für Datenschutz. Beide Funktionen können Mitarbeitern auch im Nebenamt übertragen und bei kleinen Stellen auch in einer Hand zusammengelegt werden. Grundsätzlich ist aber darauf zu achten, dass keine Interessenkollision mit sonst wahrgenommenen Aufgaben eintritt.

3.3.4 Datenschutzgerechte Löschung/Vernichtung

Sicheres Löschen magnetischer Datenträger

Sowohl aus der Sicht des Datenschutzes als auch der Informationssicherheit ist beim Löschen von sensiblen oder vertraulichen Daten (Bewohnerdaten) auf magnetischen Datenträgern zu gewährleisten, dass die Daten sicher, d. h. vollständig und unumkehrbar gelöscht werden. Einfache Löschbefehle des jeweiligen Betriebssystems oder auch das Formatieren des Datenträgers reichen hierzu in der Regel nicht aus, da eine Rekonstruktion der Daten mit frei verfügbaren Softwarewerkzeugen leicht möglich ist. Beim Löschen durch Überschreiben sind die spezifischen Besonderheiten der Verwaltung und Speicherung von Daten zu berücksichtigen, wie z. B. die Existenz von Sicherheitskopien, von automatisch durch das System oder einzelne Anwendungen angelegten temporären und Auslagerungsdateien oder von Journalen bei bestimmten Dateisystemen.

Aus Datenschutzsicht gibt es in diesem Zusammenhang die folgenden Empfehlungen:

- Der Problemkreis des sicheren Löschens von Daten erfordert die Sensibilisierung der verantwortlichen Entscheidungsträger, Administratoren, Sicherheits- und Datenschutzbeauftragten sowie jedes einzelnen Nutzers. Dies ist durch geeignete Information und Schulung zu erreichen.
- Im jeweiligen Verantwortungsbereich sind technisch-organisatorische Maßnahmen festzulegen, die eine sichere Löschung von Daten gewährleisten. Sie sind in das übergreifende Datenschutz- bzw. Sicherheitskonzept zu integrieren. Insbesondere sind Maßnahmen vor der Veräußerung, Vermietung, Aussonderung, Rückgabe, Reparatur und Wartung von Datenträgern zu bestimmen.
- Die Maßnahmen sind durch konkrete Handlungsanweisungen für das sichere Löschen zu untersetzen. Diese Anweisungen müssen den Schutzbedarf der zu löschenden Daten ebenso berücksichtigen wie den Aufwand und die Kosten für eine mögliche Datenwiederherstellung.
- Schutzwürdige Daten sind (soweit möglich) bereits in verschlüsselter Form auf dem Datenträger zu speichern. Hierzu sollten verschlüsselte Dateisysteme verwendet werden. Auch für temporäre und Auslagerungsdateien sowie für Sicherheitskopien sollten verschlüsselte Dateisysteme verwendet werden, da diese ebenfalls schutzwürdige Daten enthalten können.
- Daten auf intakten Datenträgern sind durch das ein- oder mehrmalige, komplette Überschreiben mit Zufallszahlen zu löschen. Hierbei können spezielle Softwarewerkzeuge zum Einsatz kommen. Die Verwendung gleichförmiger Überschreibmuster beim Löschen ist nicht zu empfehlen, da so kein Schutz gegen ausführliche Laboranalysen besteht.
- Das einmalige, komplette Überschreiben mit Zufallszahlen sollte beim Löschen von Daten jeder Art praktiziert werden. Die Überschreibprozedur sollte aus mindestens zwei, besser drei Durchläufen bestehen. Beim zweiten Durchlauf sollte das zum ersten Durchlauf komplementäre Muster (Bitfolge) verwendet werden. Für den dritten Durchlauf werden Zufallsdaten empfohlen. Dadurch wird eine verbesserte Schutzwirkung erzielt.
- Das selektive Löschen einzelner Dateien durch Überschreiben ist meist problematisch. Es eignet sich nur dann, wenn sichergestellt ist, dass keine Kopien der in diesen Dateien enthaltenen Daten an anderen Orten abgelegt wurden (z. B. in temporären Dateien, Auslagerungsdateien oder Sicherungskopien) oder diese Orte eindeutig bestimmt und auch die Kopien sicher gelöscht werden können. Weiter ist zu gewährleisten, dass die Metadaten der gelöschten Dateien überschrieben werden, falls sie sensible Informationen enthalten.
- Bei der Festlegung von technisch-organisatorischen Maßnahmen sowie von Handlungsanweisungen für das Löschen durch Überschreiben sind geeignete Softwarewerkzeuge anhand eines Kriterienkatalogs auszuwählen, zu bewerten und für die betreffenden Nutzer bereitzustellen. Die Anwendung der Werkzeuge ist stichprobenartig zu kontrollieren.

- Defekte Datenträger, deren Daten nicht mehr mit Softwarewerkzeugen überschrieben werden können, sind durch mechanische oder thermische Zerstörung (Disketten, Festplatten) bzw. durch magnetische Durchflutung (Disketten) unbrauchbar zu machen. Um die Zuverlässigkeit der Verfahren zu sichern, ist eine korrekte Anwendung zu gewährleisten.
- Müssen Datenträger ohne sicheres Löschen der Daten aus der Hand gegeben werden (z. B. Reparatur, Rückgabe an den Hersteller in der Garantiezeit), ist in Abhängigkeit von der Sensibilität der Daten durch vertragliche Regelungen und eventuell mit Schadensersatzansprüchen zu verhindern, dass unerwünschte Informationsflüsse stattfinden oder von Angreifern ausgenutzt werden. Gegebenenfalls ist auf Garantieansprüche zu verzichten.

Vernichten von Unterlagen

Da die Aussonderung und Vernichtung von Unterlagen (ausgefüllte Fragebögen zur Erhebung von Bewohnerdaten per Post oder durch Mitarbeiter der Stadt oder Stadtwerke) im Allgemeinen in mehreren Schritten erfolgt, sind von der Zwischenlagerung in Papierkörben oder Sammelbehältern oder dem Sammeln der Unterlagen am Arbeitsplatz über den Transport und die zentrale Deponierung bis hin zum eigentlichen Vernichtungsverfahren alle Sicherheitsaspekte zu betrachten.

Allgemeine Anforderungen

Soweit keine bereichsspezifischen Vernichtungsregelungen einschlägig sind, unterliegt die Vernichtung von Unterlagen mit personenbezogenen Daten in den öffentlichen Stellen des Bundes und im nicht-öffentlichen Bereich dem Bundesdatenschutzgesetz, ansonsten den jeweiligen Landesdatenschutzgesetzen.

Dabei sind die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um eine den Vorschriften dieses Gesetzes entsprechende Verarbeitung der Daten sicherzustellen; dies gilt auch für den Verarbeitungsschritt "Vernichtung". Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Werden personenbezogene Daten in nicht-automatisierten Dateien oder in Akten verarbeitet, sind Maßnahmen zu treffen, um insbesondere den Zugriff Unbefugter bei der Bearbeitung, der Aufbewahrung, dem Transport und der Vernichtung zu verhindern.

Grundsätzlich gilt, dass eine Stelle für die Sicherheit der Daten in Unterlagen, die vernichtet werden sollen, solange verantwortlich ist, bis die in den Unterlagen enthaltenen personenbezogenen Daten als gelöscht im Sinne

der Datenschutzgesetze gelten können, die Vernichtung also abgeschlossen ist. Die betroffene Stelle muss daher über alle Unterlagen mit personenbezogenen Daten bis zu deren Vernichtung die uneingeschränkte Verfügungsgewalt besitzen. Insbesondere dürfen zu vernichtende Unterlagen mit personenbezogenen Daten vor Abschluss der Vernichtung nicht in das Eigentum Dritter übergehen.

Der Zustand, in dem die Unterlagen als vernichtet gelten können, ist festzulegen. Als Orientierung kann hierzu die Norm DIN 66399 (Vernichten von Datenträgern) herangezogen werden. Hiernach ist eine Informationsträgervernichtung dann ausreichend, wenn die Informationsträger so vernichtet werden, dass die Reproduktion der auf ihnen wiedergegebenen Informationen nur unter erheblichem Aufwand an Personen, Hilfsmitteln oder Zeit möglich ist (Sicherheitsstufe 3).

Auch für die Vernichtung von Unterlagen gilt, dass sich die betroffene Stelle regelmäßig durch Kontrollen von der ordnungsgemäßen Durchführung der Vernichtung zu überzeugen hat. Daraus folgt, dass insbesondere dann, wenn die Vernichtung als Auftrag nach außerhalb vergeben wurde, die betroffene Stelle den gesamten technischen Vorgang oder das Verfahren kennen muss. Mit der Kontrolle der Vernichtung von Unterlagen sollte eine Person oder Organisationseinheit schriftlich beauftragt werden.

Vernichtung von Unterlagen in Eigenregie

Oberstes Prinzip sollte sein, dass Unterlagen möglichst umgehend von den Stellen vernichtet werden, die die Einstufung zur Aussonderung vornehmen. Zwischenlagerungen und Weiterreichungen über viele Hände sind fehleranfällig und erfordern genaue Regelungen und Kontrollen. Insofern ist eine unmittelbare Unterlagenvernichtung durch die zuständige Sachbearbeitung ein wirksamer Datenschutz. In jedem Fall sollte schriftlich geregelt sein, wie Mitarbeiterinnen und Mitarbeiter die Vernichtung ihrer Unterlagen durchzuführen haben. Daneben sind sie zu verpflichten, die Unterlagen bis zu deren Vernichtung sicher zu verwahren.

Werden Unterlagen zentral vernichtet, ist der gesamte Ablauf schriftlich zu regeln. Dies gilt beispielsweise für zentrale, besonders zu sichernde Sammelstellen, wie auch für den Transport zur Sammelstelle. Die Sicherheit der zu vernichtenden Unterlagen ist ebenfalls bis zu deren Ablieferung bei der Sammelstelle zu gewährleisten. Falls die Unterlagen durch einen zentralen Dienst eingesammelt werden, ist auch diese Phase unter Sicherheitsaspekten zu betrachten. Die Vernichtung der Unterlagen ist in geeigneter Weise zu protokollieren.

Vernichtung von Unterlagen durch externe Stellen

Werden Unterlagen durch externe Dritte als "**Datenverarbeitung im Auftrag**" vernichtet, ist die gesamte Handhabung und Sicherung der Unterlagen zwischen der Übergabe und dem Abschluss der Vernichtung vertraglich festzulegen. Es müssen der Transport, eine eventuell erforderliche Zwischenlagerung, der Vernichtungsort und der höchstzulässige Zeitraum zwischen der Übergabe der Unterlagen sowie dem Abschluss der Vernichtung geregelt sein. Weiter ist schriftlich festzulegen, in welchem Zustand sich die Unterlagen zu befinden haben, um als vernichtet gelten zu können. Durch den Auftragnehmer ist zu gewährleisten, dass Unbefugte keine Kenntnis der in den Unterlagen gespeicherten Daten erhalten können. Die Übergabe von Unterlagen an das Auftragsunternehmen sollte quittiert werden und die Durchführung jeder Vernichtungsaktion sollte schriftlich bestätigt werden. Generell gilt, dass die Erteilung von Unterauftragsverhältnissen möglichst ausgeschlossen werden sollte.

Die betroffene Stelle muss über ihre Unterlagen bis zum Abschluss der Vernichtung uneingeschränkt verfügen können. Die Unterlagen müssen deshalb bis zum Abschluss der Vernichtung in ihrem Eigentum bleiben. Dies beinhaltet, dass sie vor ihrer Vernichtung nicht mit fremden Unterlagen vermischt werden dürfen. Es ist deshalb auch mit dem Auftragsnehmer zu vereinbaren, dass der Auftraggeber und der zuständige Datenschutzbeauftragte bis zum Abschluss der Vernichtung zu Kontrollen berechtigt ist.

4 Literaturverzeichnis

(§ 64 BDSG 2018) § 64 BDSG. Anforderungen an die Sicherheit der Datenverarbeitung | BDSG (neu) (2018). Online verfügbar unter https://dsgvo-gesetz.de/bdsg/64-bdsg/, zuletzt aktualisiert am 05.11.2018, zuletzt geprüft am 14.11.2018.

(Art. 25 DSGVO 2018) Art. 25 DSGVO. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen | Datenschutz-Grundverordnung (DSGVO) (2018). Online verfügbar unter https://dsgvo-gesetz.de/art-25-dsgvo/, zuletzt aktualisiert am 05.11.2018, zuletzt geprüft am 14.11.2018.

(Art. 32 DSGVO 2018) Art. 32 DSGVO. Sicherheit der Verarbeitung | Datenschutz-Grundverordnung (DSGVO) (2018). Online verfügbar unter https://dsgvo-gesetz.de/art-32-dsgvo/, zuletzt aktualisiert am 05.11.2018, zuletzt geprüft am 14.11.2018.

(Art. 4 DSGVO 2018) Art. 4 DSGVO (2018). Online verfügbar unter https://dsgvo-gesetz.de/art-4-dsgvo/, zuletzt aktualisiert am 05.11.2018, zuletzt geprüft am 14.11.2018.

(Art. 5 DSGVO 2018) Art. 5 DSGVO. Grundsätze für die Verarbeitung personenbezogener Daten (2018). Online verfügbar unter https://dsgvo-gesetz.de/art-5-dsgvo/, zuletzt aktualisiert am 05.11.2018, zuletzt geprüft am 14.11.2018.

(Erwägungsgrund 026 DSGVO 2018) Erwägungsgrund 026 - EU-DSGVO. Online verfügbar unter https://www.datenschutz-grundverordnung.eu/grundverordnung/erwagungsgrund-026/, zuletzt geprüft am 14.11.2018.

(DSGVO 2018) EU-DSGVO (2018). Online verfügbar unter https://dsgvo-gesetz.de/, zuletzt aktualisiert am 05.11.2018, zuletzt geprüft am 14.11.2018.

(Kap. 3 DSGVO 2018) Kapitel 3 Artikel 12-23 (DSGVO). Rechte der betroffenen Person | Datenschutz-Grundverordnung (DSGVO) (2018). Online verfügbar unter https://dsgvo-gesetz.de/kapitel-3/, zuletzt aktualisiert am 05.11.2018, zuletzt geprüft am 14.11.2018.

5 Anhang

A.1 Aölkdsfjöaslkdjfökjasdf

DökkdHGIUEB-DFKBÖewiqwi

Bild 1:
aölskdfjöalsjdfökasjödkfjaösdfjd.

A.1.1 Aslkdjföalskdjfökasjdöf

hsdköhfeÖKFeq

A.1.2 Aälskdfjalösdf

Hksdhfwöuifqbwfe

A.2 Asdfasdf

Jlkdssnfwefwb

A.2.1 Adfasdf

Ajoenfiebcwuuwefb

A.3 Asdfasdf

Hjkasdhdqwub

A.4 Adsfasdfsdf

Jlkjupawndq