Bundesamt
für Wirtschaft und
Ausfuhrkontrolle

Energie wende
Umschalten auf Zukunft

Merkblatt Datenschutz und IT-Sicherheit

Pilotprogramm Einsparzähler

Wichtiger Hinweis auf jeweils geltende Fassung
Bitte beachten Sie: Dieses Merkblatt wird regelmäßig überarbeitet und ist jeweils nur in seiner zum Zeitpunkt der Antragstellung aktuellen Fassung für Antragsteller gültig. Regelungen und Anforderungen vorangehender oder nachfolgender Versionen haben keinerlei Gültigkeit für Antragsteller und können somit auch nicht zur Begründung oder Ablehnung von Ansprüchen geltend gemacht werden.

Der Zeitpunkt des Inkrafttretens sowie die Nummer einer Fassung sind jeweils in folgender Tabelle vermerkt:

Versionsnummer	**Datum des Inkrafttretens**
1.0	5.7.2018

An dieser Stelle finden Sie jeweils nur die aktuelle Version des Merkblatts. Zur Vermeidung von Missverständnissen werden vorangegangene Versionen entfernt. Die Speicherung der für einen Antrag jeweils maßgeblichen Fassung des Merkblatts wird Antragstellern daher empfohlen.

1. Inhaltsverzeichnis

2. Einführung

Im Rahmen des Pilotprogramms Einsparzähler geförderte Projekte sollen ein hohes Niveau von Datenschutz und Informationssicherheit gewährleisten. Das Merkblatt gibt einen Überblick über die für das Programm geltenden Mindestanforderungen, die teilweise über die gesetzlichen Vorgaben hinausgehen. Für die Erfüllung der Anforderungen sind die Antragsteller verantwortlich.

Wesentliche Datenschutz- und Informationssicherheitsanforderungen sind zusätzlich als „Erklärungen des Antragstellers“ im Antragsformular des Pilotprojekts schriftlich fixiert.

Die in diesem Merkblatt erläuterten Sachverhalte stellen grundlegende gesetzliche und spezifische Anforderungen an Datenschutz und Informationssicherheit für Einsparzählerprojekte dar. Sie sind jedoch nicht als vollständiger Leitfaden zu verstehen. Somit entbinden sie den Antragsteller nicht von seiner eigenverantwortlichen Pflicht, sich über dieses Merkblatt hinaus zu informieren und ggf. dabei zu Tage tretende zusätzliche Anforderungen abzudecken. Das BAFA garantiert weder die Aktualität, Vollständigkeit, Richtigkeit noch die Qualität der hier getroffenen Aussagen.

2.1. Begriffsbestimmungen

Im Rahmen dieses Merkblatts bezeichnet der Begriff der Informationssicherheit die Summe der Maßnahmen zum Schutz aller Informationen eines Unternehmens, wohingegen sich der Datenschutz auf die personenbezogenen Daten konzentriert (Abb. 1). Die IT-Sicherheit umfasst die technischen Aspekte und Maßnahmen des Schutzes sowohl der personenbezogenen als auch der sonstigen Daten und der Funktionsfähigkeit der IT-Systeme. Teilweise wird in der Literatur auch noch der Begriff der „Datensicherheit“ verwendet, der in Abgrenzung zur Informationssicherheit den Schutz aller Daten umfasst, manchmal aber auch nur die automatisch mit Hilfe von technischen Anlagen erfassten Daten beinhaltet.

<table>
<tr><td colspan="3">Informationssicherheit</td></tr>
<tr><td>Datenschutz</td><td>IT-Sicherheit</td><td>(Datensicherheit)</td></tr>
</table>

Abb. 1: Datenschutz und IT-Sicherheit als Teilmengen der Informationssicherheit

Im Merkblatt wird auf eine eher technische Sicht auf die Dinge abgestellt und auf den Begriff der Datensicherheit verzichtet.

2.2. Ziele und Grundwerte

Informationssicherheit umfasst den Schutz von

- Wissen (z.B. des firmeninternen Fachwissens, von Produktionsmethoden oder der Algorithmen von Software)
- Interessen (z.B. Verträgen, Vereinbarungen, aber auch der personenbezogenen Daten der Mitarbeiter und Kunden)
- Ressourcen und Infrastruktur (z.B. der technischen Funktionsfähigkeit von Maschinen und Anlagen oder IT-Systemen)
- sowie von Organisationsstrukturen (z.B. der Funktionsfähigkeit eines Unternehmens).

Das in der Verfassung verbürgte Recht auf informationelle Selbstbestimmung schützt die personenbezogenen Daten von an Einsparzählerprojekten beteiligten natürlichen Personen. Dies betrifft insbesondere die Endkunden von Einsparzählerprojekten, soweit diese natürliche Personen sind, aber z.B. auch die Mitarbeiter von Unternehmen, in denen Einsparzählerprojekte eingesetzt werden.

Für die Informationssicherheit als auch den Datenschutz gelten die gleichen Grundwerte für den Umgang von Daten:

- Vertraulichkeit,
- Integrität,
- Verfügbarkeit,
- der Schutz vor Missbrauch sowie
- die Gewährleistung der Belastbarkeit von Systemen und Diensten.

2.3. Rechtsrahmen und Anwendung auf das Pilotprogramm

Den Rechtsrahmen für Einsparzählerprojekte bilden folgende Verordnungen und Gesetze:

- Die EU-Datenschutzgrundverordnung (DSGVO), die seit dem 25. Mai 2018 unmittelbar anwendbar ist,
- Das Datenschutz-Anpassungs- und -Umsetzungsgesetz EU (DSAnpUG-EU) einschließlich des neuen Bundesdatenschutzgesetzes (BDSG-neu)

Des Weiteren kann, je nach Tätigkeit des Antragstellers, auch das „Gesetz über den Messstellenbetrieb und die Datenkommunikation in intelligenten Energienetzen“ (Messstellenbetriebsgesetz – MsbG) einschlägig sein. Obwohl sich das MsbG primär auf die Datenerhebung durch Messstellen der leitungsgebundenen Energieversorgung mit modernen Messeinrichtungen (Smart-Meter) bezieht, wird im Rahmen des Pilotprogramms seine Anwendung auch auf die Bereiche, die außerhalb des Messstellenbetriebs liegen, also auch auf das Submetering, vorgeschrieben, soweit die einzelnen Vorgaben des MsbG darauf übertragbar sind.

In Sachen Informationssicherheit werden zur Orientierung die BSI-Standards 200-1 bis 200-3 und 100-4 (künftig 200-4) zum IT-Grundschutz empfohlen. Spezielle Anforderungen des Einsparzählers werden im Abschnitt „IT-Sicherheit“ dargestellt.

2.4. Datenschutz- und IT-Sicherheit als Prozess

Datenschutz und IT-Sicherheit sind als Prozess zu verstehen. Dabei sind der Datenschutz- als auch der IT-Sicherheitsprozess weitgehend identisch. Im Merkblatt wird der Fokus auf den Datenschutz-Prozess gelegt, um Doppelungen von Anforderungen zu vermeiden. Für kleinere Fördernehmer ist in diesem Zusammenhang wichtig, dass Prozesse auch als Sub-Prozess ausgestaltet und beide Themen von einer Person betreut werden können. Es besteht auch die Möglichkeit, Verantwortung zu delegieren, z.B. an externe Dienstleister.

Der Prozess umfasst folgende Stufen

- Initialisierung des Prozesses
- Erstellung eines Konzeptes
- Realisierung fehlender Maßnahmen
- Aufrechterhaltung des laufenden Betriebs

Die Initialisierung des Prozesses beginnt mit der Benennung eines Datenschutzbeauftragten und endet mit der Erstellung des Verzeichnisses von Verarbeitungstätigkeiten. Besondere Anforderungen des Einsparzählers werden im Kapitel „Datenschutz bei der Projektkonzeption“ dargestellt.

Im Rahmen der Konzepterstellung müssen Anforderungen definiert und dabei mögliche Risiken und Gefährdungen betrachtet werden (vgl. Abschnitt Datenschutz Folgenabschätzung). Dabei sind wirtschaftliche Aspekte zu berücksichtigen. Nicht jede Gefährdung wird mit vertretbarem Aufwand vollständig zu vermeiden sein. Trotzdem ist ein hohes Maß an Sicherheit anzustreben. Spezielle Projektanforderungen des Einsparzählers sind in diesem Merkblatt definiert und auf jeden Fall zu berücksichtigen

Nicht alle der im „Verzeichnis von Verarbeitungstätigkeiten“ aufgeführten technischen und organisatorischen Maßnahmen werden auf einmal umgesetzt. Daher ist ein Zeitplan zu definieren, bis wann fehlende Maßnahmen umzusetzen sind.

Im laufenden Betrieb werden sich, z.B. durch Erweiterungen des Geschäftsmodells, Anforderungen ändern. Laufende Anforderungen des Einsparzählers werden im Kapitel „Anforderungen im Projektverlauf“ beschrieben.

3. Datenschutz - Allgemeine Anforderungen

3.1. Datenschutzbeauftragter

Soweit im Unternehmen noch nicht vorhanden, ist für Einsparzählerprojekte, abweichend von den in Art. 37 DSGVO genannten Ausnahmen, ein Datenschutzbeauftragter zu bestellen. Der Datenschutzbeauftragte muss sein Amt sachgerecht und zuverlässig ausüben können und bei der Entscheidung und Bewertung von datenschutzrelevanten Sachverhalten unabhängig sein. Die für die sachgerechte Ausübung des Amts notwendigen Kenntnisse muss sich der Datenschutzbeauftragte im Rahmen seiner Bestellung aneignen, z B. bei einer Weiterbildung. Nicht Datenschutzbeauftragte dürfen sein:

- Mitglieder der Geschäftsleitung,
- Inhaber des Unternehmens,
- EDV- und Personalverantwortliche(n),
- IT- Administratoren.

Alternativ kann ein externer Dienstleister die Rolle des Datenschutzbeauftragten übernehmen. Der Antragsteller hat dem BAFA im Rahmen der Projektskizze den Namen und die Anschrift des Datenschutzbeauftragten zu benennen.

Hinweis: Die Kosten für einen externen Datenschutzbeauftragen sind förderfähig.

3.2. Grundsätze des Datenschutzes

Für Einsparzählerprojekte gelten die Prinzipien der Datensparsamkeit bzw. Datenvermeidung und der Zweckbindung. Weiterhin gelten die Grundsätze des „Datenschutzes durch Technikgestaltung“ (data protection by design / privacy by design) sowie „Datenschutz durch datenschutzfreundliche Voreinstellungen“ (data protection by default / privacy by default).

Zweckbindung meint, dass die erhobenen Daten nur zu dem Zweck genutzt werden dürfen, für den sie erhoben worden sind. Eine zweckfremde Datenverarbeitung ist unzulässig. Der Zweck der Datenverarbeitung und -nutzung muss den Betroffenen vor der Datenerhebung mitgeteilt werden. Die Betroffenen müssen zu diesem Zweck ausdrücklich ihre Einwilligung erteilen.

Datenschutz durch Technikgestaltung: Bereits bei der Konzeption und Planung von IT-Systemen und Software sind Datenschutz und IT-Sicherheit ein wichtiger Stellenwert beizumessen. Bei der Entwicklung sind die technischen Möglichkeiten, Daten zu schützen, entsprechend dem Stand der Technik zu berücksichtigen. Dies betrifft z.B. die Notwendigkeit, Passwörter verschlüsselt zu speichern oder den Zugriff auf Daten zu authentifizieren.

Datenschutzfreundliche Voreinstellungen: IT-Systeme und Software sind so zu gestalten, dass die Prinzipien von Datensparsamkeit und Zweckbindung gewährleistet sind. So sind z.B. optionale Abfragen oder zustimmungspflichtige Zusatzangebote im Datenerhebungsprozess nicht vorauszuwählen, sondern müssen vom Nutzer aktiv ausgewählt werden.

3.3. Berechtigung zur Datenerhebung und -verarbeitung

Die Datenerhebung und -verarbeitung von personenbezogenen Daten ist nur durch den gemäß DSGVO „Verantwortlichen“ zulässig. Soweit der Antragsteller kein Messstellenbetreiber ist, wird er nur durch die **Einwilligung des Anschlussnutzers und des Endkunden** (sofern nicht identisch) hinsichtlich Zweck und Umfang der Datenerhebung berechtigt, Daten zu erheben und zu verarbeiten. Sobald ein Messstellenbetreiber Daten erhebt, die über den im MsbG festgelegten Umfang hinausgehen, hat auch dieser für die entsprechenden Daten eine Einwilligung des Anschlussnutzers und Endkunden einzuholen.

Details zur Ausgestaltung der Einwilligung werden im Kapitel „Ausgestaltung der Einwilligungserklärung“ ausgeführt. Die jeweilige Einwilligung kann nachträglich vom Einwilligenden widerrufen werden. Eine Datenerhebung und -verarbeitung ist ab diesem Zeitpunkt nicht mehr zulässig.

Es ist grundsätzlich zulässig, dass der Antragsteller die Speicherung und Verarbeitung von Daten im Rahmen einer Auftragsdatenverarbeitung an einen weisungsgebundenen externen Dienstleister auslagert. Hierbei ist sicherzustellen, dass der Antragsteller den Dienstleister auf die korrekte Einhaltung der datenschutzrechtlichen Vorgaben verpflichtet und der Dienstleister die Daten nur entsprechend der Weisungen des Auftraggebers verarbeitet. Sofern eine Auftragsdatenverarbeitung geplant ist, ist dieses im Rahmen der Projektskizze anzugeben. So die Entscheidung zur Auftragsdatenverarbeitung durch einen Dritten während der Projektlaufzeit fällt, ist dieses dem BAFA ebenfalls mitzuteilen.

3.4. Informationsrechte

Endkunden, Nutzer bzw. Anschlussnutzer haben ein Einsichtsrecht in sämtliche zu ihrer Person gespeicherten und mit ihr im Zusammenhang stehenden Daten. Soweit die Daten nicht in der Nutzeroberfläche des Endkundeninterface / Webportals des Antragstellers sichtbar sind bzw. zum Download bereitstehen, besteht ein Anspruch auf die kostenlose Weiterleitung der gespeicherten auslesbaren Daten. Soweit moderne Messeinrichtungen (mit Smart-Meter-Gateway) zum Einsatz kommen, besteht darüber hinaus das Recht, zusätzlich generierte Verbrauchsinformationen, historische Verbrauchsinformationen und, soweit der Antragsteller Energieversorger ist, Tarifinformationen einzusehen. Näheres regelt § 61 MsbG.

4. Datenschutz bei der Projektkonzeption

4.1. Risikobewertung und Datenschutz-Folgenabschätzung

Für ESZ-Projekte wird eine Risikobewertung (bzw. Gefährdungsbewertung) vorgeschrieben. Ziel ist es u.a., dass ESZ-Projekte bereits bei der Projektkonzeption die notwendigen Datenschutzaspekte hinreichend berücksichtigen und damit den Anforderungen dieses Merkblatts genügen. Soweit eine Datenverarbeitung gemäß Artikel 35 DSGVO ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen aufweist, ist zusätzlich eine Datenschutz-Folgeabschätzung vorzunehmen. Dies ist insbesondere der Fall, wenn beim Einsatz neuer Technologien große Datenmengen in hoher Auflösung verarbeitet werden, z.B. beim Einsatz von Smart-Meter-Geräten in Haushalten.

Für die Risikobewertung und Datenschutz-Folgenabschätzung können einschlägige im Internet verfügbare Leitfäden bzw. Checklisten genutzt werden. In der Regel stellen die Landesdatenschutzbeauftragten entsprechende Checklisten bereit. Die ausgefüllte Checkliste ist zu archivieren und dem BAFA auf Verlangen für die Antragsprüfung zur Verfügung zu stellen. Künftig werden die zuständigen Datenschutzbehörden Black- bzw. Whitelisten herausgeben, um Verarbeitungsvorgänge aufzulisten, bei denen auf jeden Fall beziehungsweise keine Datenschutz-Folgenabschätzung vorgenommen werden muss.

4.2. Verzeichnis von Verarbeitungstätigkeiten

Entsprechend Artikel 30 und 82 DSGVO ist der Umgang mit personenbezogenen Daten, die vom Antragsteller verarbeitet werden, im sogenannten Verzeichnis von Verarbeitungstätigkeiten zu dokumentieren. Das Verzeichnis umfasst mindestens folgende Punkte:

- Angaben zu Verantwortlichen, insbesondere Benennung und Anschrift der verantwortlichen Stelle und Kontaktdaten des Datenschutzbeauftragten,
- Zweckbestimmung der Datenerhebung, -verarbeitung oder Nutzung,
- Beschreibung der betroffenen Personengruppe und der diesbezüglichen Daten oder Datenkategorien,
- Empfänger oder Kategorien von Empfängern der Daten,
- Regelfristen für die Löschung der Daten,
- Datenübermittlung an Drittländer,
- Technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten,

Der Antragsteller stellt sicher, dass das Verzeichnis im Unternehmen existiert und die Aspekte des Einsparzählerprojekts entsprechend abbildet. Dabei kann das Einsparzählerprojekt als Sub-Verfahren dargestellt werden, wenn es nicht der einzige Unternehmensgegenstand ist. Das Verzeichnis von Verarbeitungstätigkeiten ist dem BAFA auf Verlangen zur Verfügung zu stellen.

4.3. Ausgestaltung der Einwilligungserklärung

Die Einwilligungserklärung für die Datenverarbeitung kann in den Endkundenvertrag integriert sein oder in Form eines separaten Vertrags erfolgen. Die Einwilligung hat dabei nachvollziehbar, also belegbar, zu erfolgen. Neben handschriftlich unterzeichnetes Verträgen oder Einwilligungen sind im digitalen Bereich entsprechend erteilte Opt-In's (aktivierte Checkbox) ebenfalls zulässig, sofern die Aktivierung ausreichend dokumentiert sind (Zeitpunkt und IP-Adresse). Soweit die Einwilligung in den Vertrag integriert wird, ist diese bei Verbindung mit anderen Erklärungen **hervorzuheben.** Dazu muss sich der Einwilligungstext optisch von den übrigen Erklärungen abheben und angemessen platziert sein. Die Pflicht zur Hervorhebung bezieht sich nur auf die Einwilligung selbst, nicht auf vorvertragliche Informationen. Weiterhin besteht nach DSGVO ein **Kopplungsverbot:** Der Vertragsschluss darf nicht von der Einwilligung abhängig gemacht werden, wenn dem Betroffenen ein anderer Zugang zu gleichwertigen vertraglichen Leistungen ohne die Einwilligung nicht oder nicht in zumutbarer Weise möglich ist.

Die Einwilligungserklärung beinhaltet eine umfassende **Informationspflicht**, die den Zweck der Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten betrifft. Diese Informations- und Aufklärungspflicht umfasst eine Darstellung

- der Identität der verantwortlichen Stelle,
- des Verwendungszwecks,
- der Datenverarbeitungs-Bedingungen,
- potenzieller Datenempfänger,
- der Umschreibung der betroffenen Daten,
- der Speicherdauer,

sowie der Folgen der Verweigerung der Einwilligung.

Die Einwilligungserklärung muss sich auf die Informationen über die Datenerhebung, Datennutzung, Datenverarbeitung, Datenkommunikation, Datenspeicherung und ggf. die Datenveröffentlichung beziehen. Für jeden dieser Regelungsgegenstände sind ggf. spezifisch zu definieren:

- Auf welche Datenarten bezieht sich die jeweilige Tätigkeit?
- Was ist der Verwendungszweck (Primärzweck, Kontrollzweck)?
- Wer ist Empfänger der Daten (Antragsteller, BAFA, ggf. Endkunden)?
- Findet die jeweilige Tätigkeit beim Antragsteller selbst oder bei Dritten statt?
- Wann endet die jeweilige Tätigkeit?

Soweit Endkunden und Anschlussnutzer auseinanderfallen, ist eine gesonderte Information und Zustimmung der Anschlussnutzer erforderlich, die ebenfalls die oben dargestellten Punkte umfasst.

Die im Antragsformular definierten Erklärungen (des Antragstellers) zur „Aufnahme von Endkunden" und zu „Datenschutz und Datenverwendung" sind im Rahmen der Einwilligungserklärung vollumfänglich abzubilden.

4.4. Anschlussnutzer nicht Endkunde

Wenn der Endkunde nicht der Nutzer des Einsparzählers (Anschlussnutzer) ist, sind folgende Maßgaben zu beachten:

- Eine Speicherung der Daten außerhalb der beim Nutzer befindlichen Messinfrastruktur ist nur dann zulässig, wenn der Nutzer dem ausdrücklich zustimmt. So der Nutzer der Datenerhebung nicht zustimmt, dürfen die Daten nur dann übertragen werden, wenn diese für Abrechnungszwecke (beispielsweise zur Erstellung der Heizkostenabrechnung) erforderlich sind. In diesem Fall sind die Daten lediglich in dem für Abrechnungszwecke minimal erforderlichen Umfang zu übertragen (beispielsweise ein Zählerwert am Ende des Abrechnungszeitraums).
- Verbrauchsdaten des Nutzers dürfen auch im Falle der Zustimmung zum Einsparzähler nicht an den Endkunden (beispielsweise den Vermieter) weitergegeben werden. Eine Ausnahme bilden hier lediglich die für Abrechnungszwecke benötigten Daten.
- Soweit der Einsparzähler für die Steuerung von Geräten genutzt wird (beispielsweise in Form eines smarten Thermostats), muss eine Basisfunktionalität dieser Geräte auch ohne Internetverbindung und ohne Zustimmung zur Datenweitergabe gewährleistet sein.

4.5. Auditierung des Datenschutzkonzeptes

Die Auditierung des Datenschutzkonzeptes des Einsparzählerprojekts durch ein unabhängiges Gutachten bzw. einen Datenschutzexperten ist wünschenswert, im Rahmen des Pilotprogramms Einsparzähler besteht hierzu jedoch keine Pflicht. Die im Zusammenhang mit einer Auditierung anfallenden Kosten sind förderfähig.

5. Datenschutz im Projektverlauf

5.1. Anpassungen im Projektverlauf

Soweit im Projektverlauf zusätzliche Daten erhoben oder Daten höher aufgelöst gespeichert werden, ist vorab die Zustimmung der Endkunden bzw. Nutzers einzuholen. Die Einwilligungserklärungen sind zu versionieren, um Neu- und Altkunden unterscheiden zu können.

5.2. Ausstieg von Endkunden/Nutzern

Endkunden und Nutzer haben jederzeit das uneingeschränkte Verfügungsrecht über die bei ihnen erhobenen Daten. Dies beinhaltet auch explizit das Recht, das Pilotprojekt unter angemessenen Bedingungen zu verlassen und vom Antragsteller eine Löschung der von ihm erhobenen Daten zu verlangen. Steht dem Wunsch auf Löschung kein berechtigtes Interesse entgegen, so sind die Daten unverzüglich zu löschen. Gibt es allerdinge ein berechtigtes Interesse, die Daten nicht unverzüglich zu löschen, zum Beispiel, wenn gesetzliche Aufbewahrungspflichten für Verträge und Rechnungen bestehen, so tritt an die Stelle des Anspruchs auf Löschung der Anspruch auf „Einschränkung der Verarbeitung“ gemäß Artikel 18 i. V. m. Artikel 4 Nr. 3 DSGVO. In Deutschland ist dafür auch der Begriff der „Sperrung“ gebräuchlich. Die Sperrung beinhaltet das Verbot, weitere Daten zu erheben und die vorgehaltenen Daten zu verändern oder zu nutzen. Die Sperrung gilt dann solange, bis das berechtigte Interesse erlischt. Sobald dies der Fall ist, müssen die Daten unverzüglich gelöscht werden.

Der Nachweis der leistungsabhängigen Komponente der Förderung gegenüber dem BAFA ist mit Überlassung des Datenstrings entsprechend dem Merkblatt zu „Datenerhebung und -übertragung“ gewährleistet. Die Auszahlung der leistungsabhängigen Komponente an den Antragsteller für die bei einem Endkunden erzielten Energieeinsparungen endet, wenn der Endkunde dem Antragsteller das Recht zur Speicherung und Verarbeitung von Kundendaten entzieht und ein weiterer Nachweis von Einsparungen somit nicht mehr erbracht werden kann.

5.3. Vertrags- bzw. Projektende

Nach Vertrags- bzw. Projektende sind die personenbezogenen Daten, die nicht der Aufbewahrungspflicht unterliegen, zu löschen. Schon vor diesem Zeitpunkt hat die Löschung zu erfolgen, wenn deren Speicherung für die Aufgabenwahrnehmung nicht mehr erforderlich ist. Alternativ zur Löschung ist auch eine vorherige Anonymisierung der Daten und die Weiternutzung über das Projektende hinaus möglich.

Gleiches gilt bei Betriebsstilllegungen. Bei einer Insolvenz des Antragstellers gehen alle Verpflichtungen, die den Datenschutz betreffen, auf den Insolvenzverwalter über.

6. Sonstige Anforderungen

6.1. Datenübertagung zum BAFA-Server

Zur Berechnung der Höhe der leistungsabhängigen Komponente und zur wissenschaftlichen Auswertung benötigt das BAFA Einsicht in einen Teil der Daten, die während eines Einsparzählerprojekts anfallen. Diese Daten sind vom Antragsteller auf einen von der Bewilligungsbehörde genannten Server zu übertragen. Dieses „Merkblatt zur Datenübertragung“ legt den Umfang, den Rhythmus und die Art der Übertragung fest.

Auf besonderen Antrag können die pseudonymisierten Datensätze von Endkunden von der Weitergabe zur wissenschaftlichen Auswertung ausgenommen werden, soweit begründete Datenschutzaspekte vorliegen.

6.2. Veröffentlichung von Daten

Eine Veröffentlichung personenbezogener Daten ist mit Einwilligung des Endkunden, Nutzers oder Anschlussnutzers möglich, wird aber ausdrücklich nicht empfohlen. Hintergrund dieser Empfehlung ist der Umstand, dass der Betroffene gemäß DSGVO jederzeit die Möglichkeit hat, seine Einwilligung mit Wirkung für die Zukunft zu widerrufen. Dies stellt den Verantwortlichen, der die personenbezogenen Daten veröffentlicht hat, vor die Problematik, diese wieder entfernen zu müssen. Je nach Veröffentlichungsmedium (z. B. in sozialen Medien oder regionalen Zeitungen) könnte dies schwer bis nicht hinreichend zu realisieren sein.

Soweit eine Veröffentlichung von Daten Bestandteil der Open-Source-Komponente des Antragstellers ist, ist für diese die Einwilligung des Endkunden, des Nutzers oder des Anschlussnutzers notwendig. Auch hier ist diese Einwilligung vorab mit einer Aufklärung/Information über Verwendungszweck, Ort, Dauer, Bedingungen und Einsichtsberechtigte zu verbinden.

6.3. Zusatzoption Lastmanagement-Ready

Soweit diese Zusatzoption in Anspruch genommen wird und externe Akteure (z.B. Netzbetreiber bzw. Energieversorger) Endkunden- oder Nutzeranlagen netz- oder systemdienlich steuern bzw. eine solche Steuerung erproben, dürfen die hierfür benötigten personenbezogenen Daten des Endkunden, Nutzers oder Anschlussnutzers nur mit vorab erteilter Einwilligung des Endkunden ausgetauscht werden.

7. IT-Sicherheit

7.1. Erhebung und Messung von Daten

Es gelten folgende Vorgaben:

- Smart-Meter-Gateways: Bei Verwendung von Smart-Meter-Gateways sind zur Gewährleistung der IT-Sicherheit die technischen Standards PP-0073 und TR-03109-1 des BSI einzuhalten.
- Andere fernauslesbare Messsysteme: Bei Verwendung anderer fernauslesbarer Messsysteme hat der Antragsteller dafür zu sorgen, dass die von ihm verwendete Soft- und Hardware gegen Manipulation durch Unbefugte geschützt und das Abrufen der Daten nur durch Berechtige möglich ist.
- Andere lokal auslesbare Messsysteme (beispielweise im Rahmen eines nur lokal Verfügen Energie-Management-Systems): Bei Verwendung von ausschließlich lokal auslesbaren Messsystemen hat der Antragsteller dafür zu sorgen, dass die von ihm verwendete Technik gegen Manipulation durch Unbefugte geschützt und das Abrufen der Daten nur durch Berechtigte möglich ist.

7.2. Datenübertragung

Die Datenübertragung hat verschlüsselt nach dem Stand der Technik zu erfolgen. Der Stand der Technik gilt als erfüllt, wenn die Kommunikation durch ein zertifiziertes Smart Meter Gateway entsprechend TR-03109 abgesichert wird oder wenn die Verschlüsselung der TR - 02102 des BSI genügt. Die Art der Datenübertragung und die realisierte Verschlüsselung sind im Rahmen der Projektskizze nachvollziehbar und detailliert zu beschreiben.

7.3. Datennutzung, Datenverarbeitung, Datenspeicherung

Um ein dem Risiko angemessenes Schutzniveau für die erhobenen Daten zu gewährleisten, sind gemäß Artikel 32 Abs. 1 DSGVO geeignete „technischen und organisatorischen Maßnahmen“ im Unternehmen zu treffen, zu dokumentieren und regelmäßig zu überprüfen. Dazu gehören u.a. Maßnahmen für eine hinreichende Zugangs- und Benutzerkontrolle sowie die Sicherstellung der Datenintegrität und Zuverlässigkeit der eingesetzten technischen Systeme. Eine umfassende Auflistung der betroffenen Bereiche findet sich in § 64 BDSG-neu.Soweit der Antragsteller Dritte mit dem Datenhosting beauftragt, ist die Speicherung der Daten lediglich auf dem Gebiet der Bundesrepublik Deutschland zulässig. Die die Speicherung durchführende Stelle (beispielsweise ein Rechenzentrum) muss gemäß ISO 27001 zertifiziert sein.

7.4. Endkundeninterface / Webportal

Soweit die erhobenen Daten in einer Online-Anwendung für den Endkunden bzw. Nutzer bereitgestellt werden, ist die Anwendung gegen unbefugte Nutzung, Manipulation oder Ausspähen der Daten („Hacking“) zu sichern. Daraus ergeben sich Sicherheitsanforderungen an das Web-Frontend, die Datenbank, die Netzwerkstruktur (Server), Programmierung / Updates sowie mögliche Email- und Push-Anwendungen.

Im Folgenden werden ausgewählte Detailaspekte dargestellt, die keinen Anspruch auf Vollständigkeit erheben:

Web-Frontend: Der Zugriff auf die Anwendung muss im Rahmen einer sicheren Verbindung (z.B. TLS, ehemals SSL) erfolgen und dem aktuellen Stand der Technik entsprechen. Eine Anzeige, die dem Nutzer die Komplexität/Güte des Passwortes bei der Vergabe signalisiert, ist wird empfohlen. Um eine unbefugte Nutzung zu erschweren, kann die Anzahl der Versuche, ein Passwort einzugeben, limitiert werden; der Zugriff auf die Anwendung kann auf IP-Adressen aus Deutschland beschränkt werden. Weiterhin kann eine Login-Sperre vorgesehen werden. Die Zugangsdaten dürfen nicht in Klartext auf dem jeweiligen Server hinterlegt werden (weitere Informationen unter: BSI Baustein M 4.401 – Schutz vertraulicher Daten bei Webanwendungen).

Datenbanksicherheit: Ein direkter Zugriff auf die Datenbank bei der Datenverarbeitung sollte vermieden werden. Die Nutzung eines Backend wird empfohlen. Bei personenbezogenen Daten ist eine verschlüsselte und von den Verbrauchsdaten getrennte Speicherung in der Datenbank anzustreben.

Netzwerkstruktur: Auch bei Root-Zugriff für den Server sind die Passwortkonventionen einzuhalten. Die Ausspielung von Fehlern in der Endkundenanwendung ist zu deaktivieren.

Programmierung: Die Verwendung eines Frameworks für die Programmierung erhöht die Sicherheit.

7.5. Wartung, Aufrechterhaltung der Funktionsfähigkeit / Notfallmodus

Der Fördernehmer muss in der Lage sein, die von ihm installieren Geräte, wenn notwendig (beispielsweise bei Bekanntwerden von Sicherheitslücken), zu warten. Die dafür nötigen Zugänge sind adäquat abzusichern.

Einsparzähler sind so zu gestalten, dass deren Hard- und Softwarekomponenten langlebig und wenig störanfällig sind. Datenverlusten, z.B. durch Strom- oder Internetausfall, ist vorzubeugen. So ist es z.B. möglich, Datenverluste durch Vorhaltung einer hohen Speichertiefe vor Ort mittels Speicherkarten oder einer Ringspeicherung vorzubeugen.

Für Ausfälle der Internetverbindung ist ein Notfall-Modus vorzusehen, der den Nutzer in die Lage versetzt, wesentliche Funktionen, die für die Steuerung von Geräten genutzt werden, vor Ort aufrecht zu erhalten. Hierfür sind hardwarebasierte Notfallsysteme oder alternative Regelmechanismen vorzuhalten. Lösungsansätze für alternative Regelmechanismen können sein: ein Rückfall auf die lokale Regelung, Relais-Schaltungen oder die mehrmalige Wiederholung eines Schaltbefehls. Möglich ist auch der Einsatz eines Störmeldungsmanagements.

8. Meldepflichten / Sanktionen

Der Antragsteller ist zur Einhaltung der gesetzlichen Anforderungen zum Datenschutz, der Anforderungen aus diesem Merkblatt sowie der eigenen Endkunden- bzw. Nutzervereinbarungen verpflichtet. Die Sicherheit der IT-Systeme, die für das Einsparzählerprojekt genutzt werden, ist zu gewährleisten und kontinuierlich zu verbessern. Soweit der Antragsteller im Projektverlauf Lücken im Datenschutz bzw. bei dessen technischer Umsetzung (z.B. Sicherheitslücken) feststellt, hat er diese eigenständig unverzüglich zu schließen. Die ergriffenen Maßnahmen sind zu dokumentieren.

Eingetretene Datenschutz-/sicherheitsrelevante Ereignisse (z.B. erfolgreiche Hackerangriffe), die mit einer Verletzung der Sicherheit der personenbezogenen Daten und einem Risiko für die Rechte und Freiheiten natürlicher Personen verbunden sind, sind gemäß den Artikeln 33 und 34 DSGVO der zuständigen Datenschutz-Aufsichtsbehörde und zusätzlich dem BAFA unverzüglich und möglichst innerhalb von 72 Stunden zu melden. Besteht ein hohes Risiko für die betroffenen Personen, hat der Fördernehmer diese ebenfalls zu informieren.

9. Glossar

- **Personenbezogene Daten:** Personenbezogen Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Zu den personenbezogenen Daten im Sinne des Pilotprogramms gehören alle Daten, die ggf. auch mit Zusatzwissen ein Wiedererkennen zum Zeitpunkt der Datenerhebung ermöglichen, also auch Daten mit indirekt bestimmbarem Personenbezug und pseudonymisierte Daten. Im Sinne des Einsparzählers sind Daten, die einem Haushalt zugeordnet werden können, personenbezogene Daten.
- **Submetering:** Unter Submetering wird die verbrauchsabhängige Erfassung und Verteilung von Energie verstanden, an der Energieversorger und Messstellenbetreiber nicht beteiligt sind. Eine typische Anwendung von Submetering ist die Abrechnung der Heiz- und Wasserkosten in Gebäuden. Bei der Heiz- und Warmwasserkostenabrechnung umfasst das Submetering auch die messtechnische Ausstattung der Mieteinheiten mit Heizkostenverteilern oder Wärme- und Wasserzählern sowie die Erstellung der Abrechnung selbst.
- **Pseudonymisierte Daten:** Daten, bei denen der Personenbezug codiert ist, z.B. durch eine Nummer. Mit Hilfe des Codes kann der Personenbezug wiederhergestellt werden.
- **Anonymisierte Daten:** Es ist kein Personenbezug vorhanden bzw. dieser kann auch nicht mit Zusatzwissen widerhergestellt werden.
- **Anschlussnutzer** entsprechend MsbG**:** Der zur Nutzung des Netzanschlusses berechtigte Letztverbraucher oder Betreiber von Erzeugungsanlagen.
- **Endkunde:** Vertragspartner des Antragstellers für ein Einsparzähler-Projekt, i.d.R. auch Anschlussnutzer
- **Nutzer:** Nutzer des Einsparzählers, aber nicht Endkunde und damit Vertragspartner des Antragstellers ist, z.B. Einsparzählerprojekt zu Raumwärme mit Mietern in einem Mehrfamilienhaus.
- **Messsystem:** Eine in ein Kommunikationsnetz eingebundene Messeinrichtung
- **moderne Messeinrichtung** entsprechend MsbG: Eine Messeinrichtung, die den tatsächlichen Elektrizitätsverbrauch und die tatsächliche Nutzungszeit widerspiegelt und über ein Smart-Meter-Gateway sicher in ein Kommunikationsnetz eingebunden werden kann.

Impressum

Herausgeber
Bundesamt für Wirtschaft und Ausfuhrkontrolle
Leitungsstab Presse- und Öffentlichkeitsarbeit
Frankfurter Str. 29 - 35
65760 Eschborn

http://www.bafa.de/

Referat: 5.11
E-Mail: esz@bafa.bund.de

Tel.: +49(0)6196 908-2114
Fax: +49(0)6196 908-800

Stand
5.07.2018

Bildnachweis

Das Bundesamt für Wirtschaft und Ausfuhrkontrolle ist mit dem audit berufundfamilie für seine familienfreundliche Personalpolitik ausgezeichnet worden. Das Zertifikat wird von der berufundfamilie GmbH, einer Initiative der Gemeinnützigen Hertie-Stiftung, verliehen.