

# Data Protection Impact Assessment / Datenschutz-Folgenabschätzung für den Smart Meter Einsatz

White Paper

Revision 1.4

## Revisionsverlauf

| Datum         | Revision | Änderung                                              | Verantwortlich         |
|---------------|----------|-------------------------------------------------------|------------------------|
| 1. Juni 2017  | Rev. 0.1 | Erstellung                                            | Dr. Manfred Stallinger |
| 7. Juni 2017  | Rev. 1.0 | Überarbeitung und Freigabe zur Diskussion             | Dr. Manfred Stallinger |
| 18. Juni 2017 | Rev. 1.1 | Einarbeitung Feedback                                 | Dr. Manfred Stallinger |
| 8. Juli 2017  | Rev. 1.2 | Einarbeitung der Aspekte aus dem Meeting v. 5.7.2017  | Dr. Manfred Stallinger |
| 13. Juli 2017 | Rev. 1.3 | Einarbeitung der Aspekte aus dem Meeting v. 13.7.2017 | Dr. Manfred Stallinger |
| 15. Juli 2017 | Rev. 1.4 | Übersicht der PIA-Werte eingefügt                     | Dr. Manfred Stallinger |

## Inhaltsverzeichnis

|      |                                                                                                                     |    |
|------|---------------------------------------------------------------------------------------------------------------------|----|
| 1    | Zielsetzung.....                                                                                                    | 4  |
| 2    | Begriffsbestimmungen.....                                                                                           | 4  |
| 2.1  | Verarbeitungstätigkeit.....                                                                                         | 4  |
| 2.2  | Datenschutz-Folgenabschätzung - Data Privacy Impact Assessment (DPIA).....                                          | 4  |
| 2.3  | Risikobeurteilung im Data Privacy Impact Assessment.....                                                            | 5  |
| 2.4  | Beurteilung der potentiellen Gefährdung des Betroffenen.....                                                        | 5  |
| 2.5  | Kriterien zur Beurteilung der Folgen für betroffene natürliche Personen.....                                        | 6  |
| 3    | Abgrenzung und Scope.....                                                                                           | 7  |
| 3.1  | Liste der Verarbeitungstätigkeiten im Smart Metering Prozess.....                                                   | 8  |
| 4    | Erfordernis der Durchführung einer DPIA.....                                                                        | 8  |
| 4.1  | Kriterien für eine verpflichtende Durchführung der DPIA.....                                                        | 8  |
| 4.2  | Entscheidungsbaum.....                                                                                              | 10 |
| 5    | Strukturierung eines DPIA-Modells.....                                                                              | 11 |
| 6    | Berichterstattung.....                                                                                              | 12 |
| 7    | Beurteilung der Bedrohung Betroffener.....                                                                          | 13 |
| 7.1  | Kundeninfo über bevorstehenden SM-Einbau.....                                                                       | 13 |
| 7.2  | Zählerumstellung auf intelligentes Messgerät (IMS oder IME).....                                                    | 13 |
| 7.3  | Parametrisierung des DSZ (dig. Standardzähler).....                                                                 | 13 |
| 7.4  | Parametrisierung des IMS (Erstmaliges Laden bzw. Änderung eines Parametersatzes).....                               | 14 |
| 7.5  | Parametrisierung des IME (Erstmaliges Laden bzw. Änderung eines Parametersatzes).....                               | 14 |
| 7.6  | Ablesung der 14 Stundenwerte am Zähler am Meterdisplay durch den Kunden oder Vertreter.....                         | 14 |
| 7.7  | Automatisierte Auslesung der DSZ (dig. Standardzähler) entsprechend der ELWOG Vorgaben durch den Netzbetreiber..... | 15 |
| 7.8  | Automatisierte Auslesung des IMS entsprechend der ELWOG Vorgaben durch den Netzbetreiber.....                       | 15 |
| 7.9  | Automatisierte Auslesung des IME entsprechend der ELWOG Vorgaben durch den Netzbetreiber.....                       | 15 |
| 7.10 | 10. Manuelle Auslesung eines elektronischen Messgerätes.....                                                        | 16 |
| 7.11 | Bereitstellung der Verbrauchsdaten am Kundenportal.....                                                             | 16 |
| 7.12 | Kundenanmeldung.....                                                                                                | 16 |
| 7.13 | Kundenabmeldung.....                                                                                                | 16 |
| 7.14 | Marktkommunikation Lieferant.....                                                                                   | 17 |
| 7.15 | Telefonauskunft.....                                                                                                | 17 |
| 7.16 | Abschaltung.....                                                                                                    | 17 |
| 7.17 | Wiederinbetriebnahme nach einer Abschaltung.....                                                                    | 18 |
| 7.18 | Anforderung an Prepayment.....                                                                                      | 18 |
| 8    | Glossar.....                                                                                                        | 19 |

# 1 Zielsetzung

Die Datenschutz-Grundverordnung (DSGVO) ist eine Verordnung der Europäischen Union, die jede Verarbeitung von personenbezogenen Daten durch private Unternehmen und öffentliche Stellen in der Union vereinheitlicht. Dadurch soll sowohl der Schutz von personenbezogenen Daten innerhalb, als auch der Datenverkehr außerhalb der Union sichergestellt und durch Regulative geregelt werden. Diese Verordnung ersetzt die aus dem Jahr 1995 stammende Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten.

Das Data Privacy Impact Assessment ("DPIA") ist das zentrale Element der Datenschutzgrundverordnung. Mit dieser Folgenabschätzung wird die potentielle Bedrohung (Risiko) der natürlichen Person aus der Verarbeitung seiner personenbezogenen Daten festgestellt. Diese Beurteilung der potentiellen Folgen ist im Rahmen eines kontinuierlichen Prozesses zyklisch durchzuführen.

Die zentrale Aufgabe des Data Privacy Impact Assessments ("DPIA") ist es, Gefahren zu identifizieren, die eine nennenswerte Einschränkung der Rechte und Freiheiten der natürlichen Person nach sich ziehen könnten. Im Kontext der Anwendung von Smart Meter zur Auslesung von Verbrauchswerten wird die Datenschutz-Folgenabschätzung auf den privaten Stromkunden als Konsument (Consumer) bzw. Konsument und Stromerzeuger (Producer) als natürliche Person reduziert.

Das gegenständliche, von der Arbeitsgruppe DPIA-Smart Meter bei Österreichs Energie entwickelte Verfahren zur Durchführung einer Datenschutz Folgenabschätzung inklusive der Verhaltensregeln für Netzbetreiber bei der Verwendung von mit intelligenten Messgeräten erhobenen personenbezogenen Daten von Endverbrauchern, ist eine direkte Ableitung der, von der Smart Grid Task Force, Expert Group 2 vorgeschlagenen Vorgehensweise.

## 2 Begriffsbestimmungen

### 2.1 Verarbeitungstätigkeit

Der Begriff „Verarbeitungstätigkeit“ bezeichnet die Gesamtheit an Tätigkeiten, mit deren Hilfe eine Zweckbestimmung oder ein Bündel zusammengehöriger Zweckbestimmungen realisiert wird. Eine Verarbeitungstätigkeit kann auf mehrere Datenstämme aufsetzen und zur Verarbeitung unterschiedliche DV-Programmen und Dateien nutzen. Wesentlich für die Bestimmung einer Verarbeitungstätigkeit ist der mit dieser Tätigkeit verfolgte und eindeutige Zweck der Datenverarbeitung.

### 2.2 Datenschutz-Folgenabschätzung - Data Privacy Impact Assessment (DPIA)

Die Datenschutz-Folgenabschätzung entspricht im Wesentlichen einer proaktiven „Vorabkontrolle“ der geplanten Verarbeitung bezogen auf mögliche Einflüsse auf Recht und Freiheit des Betroffenen. Diese DPIA ist immer dann durchzuführen, wenn besonders schützenswerte Daten nach Art. 9 bzw. Art. 10 EU-DSGVO verarbeitet werden oder die Verarbeitung dazu bestimmt ist, die Persönlichkeit des Betroffenen, einschließlich seiner Fähigkeiten, Leistungen oder seines Verhaltens zu überwachen.

In diesen Fällen sind die in der Verarbeitungstätigkeit innewohnenden Risiken für eine Einschränkung der Rechte und Freiheiten des Betroffenen zu evaluieren. Die Risiken für eine mögliche Einschränkung der Rechte und Freiheiten des Betroffenen werden nach den Kriterien der Verfügbarkeit, Vertraulichkeit und Integrität (Richtigkeit) der personenbezogenen Daten, der Nichtverkettbarkeit einzelner Datenarten sowie der Transparenz und Interventionierbarkeit im Prozess der Datenverarbeitung beurteilt.

## 2.3 Risikobeurteilung im Data Privacy Impact Assessment

Im angewandten Verfahren zum Management des Datenschutz-Prozesses (DSMS) wird eine Beurteilungslogik zugrunde gelegt, die dem verantwortlichen Auftraggeber der Datenverarbeitung eine Einschätzung der möglichen Risiken für den Betroffenen erlaubt. Diese Beurteilung erfolgt anhand eines bekannten Scoring-Modelles auf Basis der Kennzahlen aus der Versicherungswirtschaft. Diese sind wie folgt zu interpretieren:

| Kennzahl | Interpretation                                                                                                                                                                                                                                                                                                                |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AAA      | Dem Betroffenen erwachsen aufgrund bestmöglicher technischen und organisatorischen Vorkehrungen in der Verarbeitung oder aufgrund der nicht erkennbaren Auswirkung aus der Verarbeitung seiner personenbezogenen Daten keine Einschränkung in seinen Rechten und seiner Freiheit.                                             |
| AA       | Dem Betroffenen erwachsen aufgrund der sehr guten technischen und organisatorischen Vorkehrungen in der Verarbeitung oder aufgrund der unwesentlichen Auswirkung aus der Verarbeitung seiner personenbezogenen Daten keine erkennbare Einschränkung in seinen Rechten und seiner Freiheit.                                    |
| A        | Dem Betroffenen erwachsen aufgrund der über dem „Üblichen“ hinausgehenden technischen und organisatorischen Vorkehrungen in der Verarbeitung oder aufgrund der geringen Auswirkung aus der Verarbeitung seiner personenbezogenen Daten nur unwesentliche Einschränkungen in seinen Rechten und seiner Freiheit.               |
| BBB      | Dem Betroffenen erwachsen aufgrund der ordnungsgemäßen technischen und organisatorischen Vorkehrungen in der Verarbeitung oder aufgrund der Auswirkungen aus der Verarbeitung seiner personenbezogenen Daten keine, über ein normales Maß hinausreichende Einschränkung in seinen Rechten und seiner Freiheit.                |
| BB       | Dem Betroffenen erwachsen aufgrund der technischen und organisatorischen Vorkehrungen in der Verarbeitung und aufgrund der Auswirkungen aus der Verarbeitung seiner personenbezogenen Daten ein, über ein normales Maß hinausreichende Einschränkung in seinen Rechten und seiner Freiheit.                                   |
| B        | Dem Betroffenen erwachsen aufgrund der mangelhaften technischen und organisatorischen Vorkehrungen in der Verarbeitung und aufgrund der schweren Auswirkungen aus der Verarbeitung seiner personenbezogenen Daten eine wesentliche Einschränkung in seinen Rechten und seiner Freiheit.                                       |
| CCC      | Dem Betroffenen erwachsen aufgrund der nur in Ansätzen vorhandenen technischen und organisatorischen Vorkehrungen in der Verarbeitung und aufgrund der besonders schweren Auswirkungen aus der Verarbeitung seiner personenbezogenen Daten eine wesentliche Einschränkung in seinen Rechten und seiner Freiheit.              |
| DEFAULT  | Dem Betroffenen erwachsen aufgrund der nicht vorhandenen technischen und organisatorischen Vorkehrungen in der Verarbeitung und aufgrund der sehr großen Auswirkung aus der Verarbeitung seiner personenbezogenen, sensiblen Daten eine nachhaltige und sehr wesentliche Einschränkung in seinen Rechten und seiner Freiheit. |

Tabelle 1: Scoringmodell zur Risikobeurteilung im Rahmen der Datenschutz-Folgenabschätzung

Die Tabelle beschreibt die Risikokennzahl anhand der aus Ratingmodellen bekannten Buchstabenkombinationen „AAA“ bis „Default“. „AAA“ beschreibt dabei das höchste, „Default“ das niedrigste. Der Wert des „BBB“ beschreibt jenen Wert, der dem Stand der Technik bzw. der angewandten Praxis entspricht. Ein einfaches „BB“ kann dabei als unterhalb der üblichen Praxis bzw. „B“ als leicht fahrlässig beschrieben werden. Ein „CCC“ oder „Default“ eine wesentliche Abweichung vom Stand der Technik und beschreibt eine grobe Fahrlässigkeit.

Kennzahlen von „A“ bis „AAA“ beschreiben eine Übererfüllung der vom Stand der Technik geforderten Umsetzung. Dies kann insbesondere bei der Anwendung neuester Technologien in den ersten Jahren, bis der Markt diese Technologien als die übliche Praxis anerkennt, der Fall sein.

## 2.4 Beurteilung der potentiellen Gefährdung des Betroffenen

Im angewandten Verfahren zum Management des Datenschutz-Prozesses (DSMS) wird der Beurteilungslogik auch eine Beurteilung des Grads der potentiellen Gefährdung des Betroffenen, ein „Privacy Impact Assessment“ (PIA) zugrunde gelegt. Diese PIA erfasst die für die Datenschutz-Folgenabschätzung erforderlichen Dimensionen der möglichen Gefährdung für den Betroffenen. Aus den vorhandenen technischen und organisatorischen Vor-

kehrungen für die Verarbeitung der personenbezogenen Daten und dem Ergebnis aus dem Privacy Impact Assessment wird die Scoring Kennzahl (siehe Risikobeurteilung in der Datenschutz-Folgenabschätzung) ermittelt. Die Beurteilungskriterien in der PIA sind wie folgt zu interpretieren:

| Grad der Gefährdung | Interpretation                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| unbedeutend         | Es werden personenbezogene Daten verarbeitet, die bereits öffentlich sind oder auch durch zulässige Recherchen zu erwerben sind.                                                                                                                                                                                                                                                                                   |
| gering              | Es werden personenbezogene Daten verarbeitet, die nicht öffentlich und auch nicht durch zulässige Recherchen zu erwerben sind und auch keine erkennbaren Konsequenzen für den Betroffenen zu erwarten sind.                                                                                                                                                                                                        |
| mittel              | Es werden personenbezogene Daten verarbeitet, ohne dass wesentliche und nachhaltige Konsequenzen für den Betroffenen zu erwarten sind.                                                                                                                                                                                                                                                                             |
| hoch                | Es werden personenbezogene (Profiling-) Daten (Art. 35 Abs. a EU-DSGVO) und/oder Daten, die ein hohes Schutzbedarft (Artikel 9 bzw. 10 EU-DSGVO) aufweisen, verarbeitet. Der Betroffene ist von den Entscheidungen bzw. Leistungen des verantwortlichen Auftraggebers der Verarbeitung unmittelbar abhängig. Die Gefährdung aus der Datenverarbeitung kann zu erheblichen Konsequenzen für den Betroffenen führen. |
| sehr hoch           | Es werden personenbezogene Daten (Artikel 9 bzw. 10 (EU-DSGVO) mit hohem Schutzbedarf verarbeitet. Darüber hinaus ist der Betroffene von den Entscheidungen bzw. Leistungen des verantwortlichen Auftraggebers der Verarbeitung unmittelbar existenziell abhängig.                                                                                                                                                 |

**Tabelle 2: Beurteilungskriterien im Privacy Impact Assessment (PIA)**

## 2.5 Kriterien zur Beurteilung der Folgen für betroffene natürliche Personen

Zur Beurteilung der Folgen für betroffene natürliche Personen werden sechs Beurteilungskriterien zugrunde gelegt. Damit die Semantik dieser Beurteilungskriterien eindeutig interpretiert werden können, werden die Begriffe nachfolgend im Kontext dieses White Papers definiert.

### 2.5.1 Verfügbarkeit

Das Kriterium der Verfügbarkeit von Daten ist ein Maß für die Wahrscheinlichkeit, dass bestimmte Daten zu einem bestimmten Zeitpunkt der betroffenen natürlichen Personen zur Verfügung stehen.

### 2.5.2 Vertraulichkeit

Vertraulichkeit ist die Eigenschaft einer Information, nur einem beschränkten, klar festgelegten Empfängerkreis vorgesehen zu sein. Eine Weitergabe und Veröffentlichung ohne Zustimmung des Informationseigentümers ist nicht zulässig.

### 2.5.3 Integrität (Unversehrtheit)

Das Kriterium der Integrität von Daten beschreibt eine Eigenschaft von Daten / Informationen, dass diese ohne Zustimmung des Informations- bzw. Dateneigentümers nicht durch eine unzulässige Verarbeitung verändert oder gelöscht wurden.

### 2.5.4 Nichtverkettbarkeit (Zweckbindung / Zwecktrennung)

Das Kriterium der Nichtverkettbarkeit beschreibt eine Eigenschaft von Verarbeitungen personenbezogener Daten, diese nicht oder nur mit unverhältnismäßig hohem Aufwand für einen anderen als den ausgewiesenen Zweck durch Verknüpfung (Verkettung) der Dateninhalte erheben, verarbeiten und nutzen zu können.

### 2.5.5 Transparenz (Nachvollziehbarkeit)

Das Kriterium der Transparenz beschreibt eine Eigenschaft von Verarbeitungen personenbezogener Daten, die der betroffenen natürlichen Person die Möglichkeit gibt, die Verarbeitung mit zumutbarem Aufwand nachvollziehen und überprüfen zu können.

### 2.5.6 Intervenierbarkeit (Eingreifbarkeit)

Das Kriterium der Intervenierbarkeit beschreibt eine Eigenschaft von Verarbeitungen personenbezogener Daten, die der betroffenen natürlichen Person die Möglichkeit gibt, die Ausübung der ihm zustehenden Rechte wirksam durchsetzen zu können.

## 3 Abgrenzung und Scope

In der Arbeitsgruppe DPIA für Smart Meter bei Österreichs Energie (ÖE) wird mit dem gegenständlichen Verfahren eine Vorgehensweise festgelegt, mit der die Einhaltung, insbesondere die Abschätzung der Folgen aus der Verarbeitung von personenbezogener Daten (Art. 35 EU-DSGVO) für den Betroffenen als natürliche Person durchgeführt werden kann.

Dazu wird festgehalten, dass die Smart Meter Infrastrukturen Teil der gesamten (kritischen) IT-Systemlandschaft bei Energieversorgern bzw. Netzbetreibern sind. Für die gesamten kritischen IT-Infrastrukturen ist der Betreiber dieser Infrastrukturen auch verpflichtet ein Informationssicherheits-Managementsystem (ISMS) zu betreiben. Diese Informationssicherheit ist Teil der der Forderung aus der Datenschutz-Grundverordnung (Artikel 32).

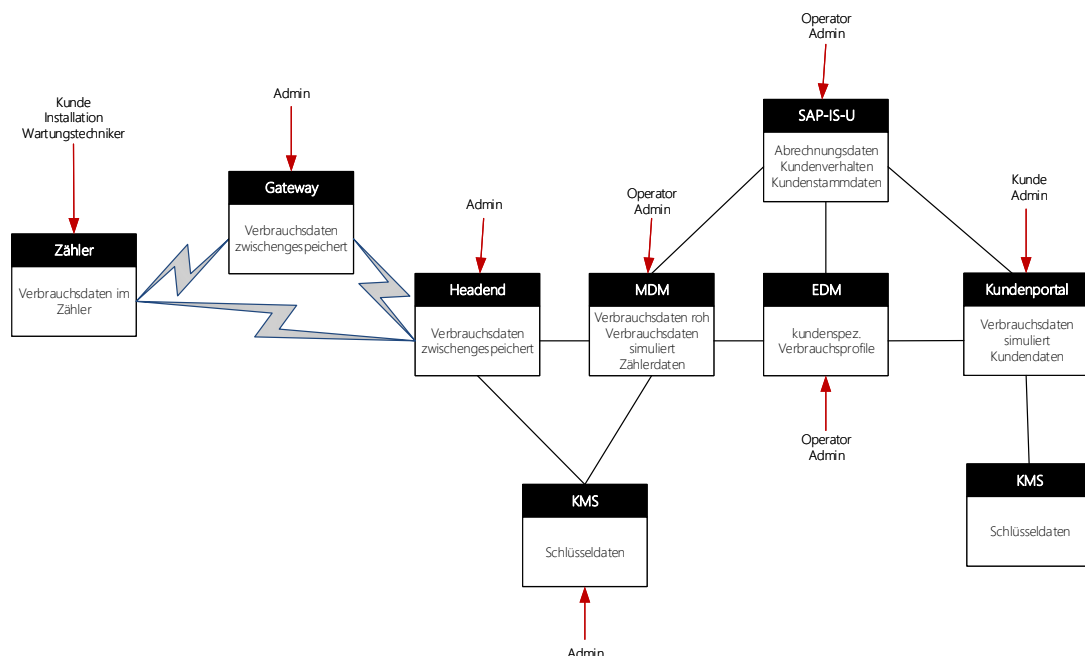


Abbildung 1: Layout der SM Infrastruktur

Ein wesentlicher Anteil der von diesem ISMS erfassten IT-Infrastrukturen sind auch Basis der Smart Meter Infrastruktur. Dennoch sind in der Betrachtung der DPIA bei Smart Metern Systemgrenzen zur übrigen IT-Systemlandschaft einzuziehen. Aus diesem Grund wurde der Scope einvernehmlich auf die in der Abbildung 1 dargestellten Infrastruktur und auf den Endkunden als natürliche Person reduziert.

In der EU-DSGVO ist generell der Scope auf alle betroffenen natürlichen Personengruppen, die im Unternehmen von Verarbeitungstätigkeiten mit Personenbezug betroffen sind, festgesetzt. Daher sind alle über den hier gegenständlich festgelegten Scope im Smart Metering hinausreichende Verarbeitungen von personenbezogenen Daten, in einem generellen Datenschutzmanagement des Unternehmens abzudecken.

### 3.1 Liste der Verarbeitungstätigkeiten im Smart Metering Prozess

Im Rahmen der Identifikation der Verarbeitungstätigkeiten im Smart Metering Prozess wurden nachfolgende Tätigkeiten bzw. Teilprozesse identifiziert (siehe Tabelle 3)

| Nr. | Verarbeitungstätigkeit                                                                                                    |
|-----|---------------------------------------------------------------------------------------------------------------------------|
| 1   | Kundeninfo über bevorstehenden SM-Einbau                                                                                  |
| 2   | Zählerumstellung auf intelligentes Messgerät (IMS oder IME) (Arbeitsvorbereitung, Montage und Inbetriebnahme beim Kunden) |
| 3   | Parametrisierung des DSZ (dig. Standardzähler) (Erstmaliges Laden bzw. Änderung eines Parametersatzes)                    |
| 4   | Parametrisierung des IMS (Erstmaliges Laden bzw. Änderung eines Parametersatzes)                                          |
| 5   | Parametrisierung des IME (Erstmaliges Laden bzw. Änderung eines Parametersatzes)                                          |
| 6   | Auslesung der ¼ Stundenwerte am Zähler am Meterdisplay durch den Kunden oder Vertreter                                    |
| 7   | Automatisierte Auslesung der DSZ (dig. Standardzähler) entsprechend der ELWOG Vorgaben durch den Netzbetreiber            |
| 8   | Automatisierte Auslesung des IMS entsprechend der ELWOG Vorgaben durch den Netzbetreiber                                  |
| 9   | Automatisierte Auslesung des IME entsprechend der ELWOG Vorgaben durch den Netzbetreiber                                  |
| 10  | Bereitstellung der Verbrauchsdaten am Kundenportal                                                                        |
| 11  | Kundenanmeldung                                                                                                           |
| 12  | Kundenabmeldung                                                                                                           |
| 13  | Marktkommunikation Lieferant                                                                                              |
| 14  | Telefonauskunft                                                                                                           |
| 15  | Abschaltung                                                                                                               |
| 16  | Wiederinbetriebnahme nach einer Abschaltung                                                                               |
| 17  | Anforderung an Prepayment                                                                                                 |

Tabelle 3: Liste der Verarbeitungstätigkeiten im Smart Metering Prozess

## 4 Erfordernis der Durchführung einer DPIA

Die Datenschutz-Grundverordnung (DSGVO) sieht eine verpflichtende Durchführung einer Datenschutz-Folgenabschätzung vor, sofern bestimmte Kriterien erfüllt sind. Im Unterabschnitt 4.1 „Kriterien für eine verpflichtende Durchführung der DPIA“ sind diese Kriterien näher beschrieben. Im Unterabschnitt 4.2 „Entscheidungsbaum“ ist ein Entscheidungsbaum dargestellt, der im Durchlauf zu einem Ergebnis „DPIA ist NICHT erforderlich“ bzw. „DPIA IST erforderlich“ führt.

### 4.1 Kriterien für eine verpflichtende Durchführung der DPIA

Kriterium 1: Sind personenbezogene Daten involviert?

- Werden mit dem Programm personenbezogene Daten verarbeitet?
- Werden Daten aus dem Programm mit personenbezogenen Daten von außerhalb verknüpft?

- Können die gesammelten Daten durch die Verknüpfung durch Dritte zu personenbezogenen Daten werden?
- Werden durch das Programm personenbezogene Daten von anderen Systemen erfasst?
- Enthält das Programm andere Maßnahmen, die die Privatsphäre beeinträchtigen können?

Kriterium 2: Verantwortliche / Auftragsverarbeiter

- Werden personenbezogene Daten im Auftrag einer anderen Organisation nach deren Anforderungen verarbeitet?
- Sicherheits- und Datenschutzerfordernungen sind in der Beziehung zwischen Verantwortlichen und Verarbeiter definiert?

Kriterium 3: Auswirkungen auf Rechte und Freiheit

- Sind die Impacts auf den Betroffenen ihrer Organisation bekannt?
- Verliert der Betroffene die Kontrolle über seine personenbezogenen Daten?
- Sind die Betroffenen in der Lage zu kontrollieren, welche Daten gesammelt werden?
- Sind die Betroffenen in der Lage, ihre Daten zu kontrollieren, nachdem sie gesammelt / verarbeitet worden sind?
- Ist zu erwarten, dass die Betroffenen nachdem ihre personenbezogenen Daten gesammelt wurden, ihr Verhalten ändern werden (z. B. Energieverbrauch oder Versorgungswechsel -das Recht auf freie Wahl könnte gefährdet werden)?

Kriterium 4: Wann sollte ein DPIA durchgeführt werden (richtiges Timing und Motivation)

- Es wird ein neues Programm, eine neue Dienstleistung im Rahmen einer Verarbeitungstätigkeit oder eine neue Verarbeitungstätigkeit (Verfahren) entwickelt.
- Es werden wesentliche Änderungen an einer vorhandenen Verarbeitungstätigkeit vorgenommen.
- Es wird eine Verarbeitungstätigkeit durchgeführt, ohne dass eine DPIA durchgeführt wurde?
- Bei einer Datenverletzung.
- Wenn ein cloudbasierter Dienst für die Verarbeitungsvorgänge mit personenbezogenen Daten verwendet werden soll.

Kriterium 5: Art der System- / Anwendungsübung

Zweck:

- Ist der Zweck der Erhebung der persönlichen Daten nicht klar oder nicht mit den Betroffenen vereinbart?
- Werden die durch das Programm erhobenen personenbezogenen Daten, zu abweichenden, einschließlich Forschung und statistischen Zwecken verwendet?
- Beeinflusst der Zweck der Verarbeitung die Privatsphäre?
- Werden die Daten für Profiling verwendet?

System:

- Wird der Einsatz oder der Zweck der verwendeten Technologie oder der Zweck des Programms Fragen und / oder Widerstand von den Betroffenen aufwerfen?
- Sollten neue noch unbekannte Technologien zum Einsatz kommen?

Organisatorisches:

- Sind die Rollen und Verantwortlichkeiten für die Verarbeitung der personenbezogenen Daten unklar?
- Wird die Verarbeitung personenbezogener Daten von einem Auftragsverarbeiter durchgeführt?
- Werden die personenbezogenen Daten an andere Organisationen weitergegeben?

Kriterium 6: Rechtsgrundlage und Besorgnis der Öffentlichkeit

- Gibt es eine gesetzliche Verpflichtung zur Durchführung einer Datenschutzfolgenabschätzung?
- Ist die Rechtsgrundlage für die Verarbeitung von Verbrauchsdaten noch nicht bestimmt?
- Gibt es einen rechtlichen Rahmen für die Anwendung oder den Smart-Grid-Use-Case?
- Werden Bedenken der Öffentlichkeit für die Verarbeitung hinsichtlich der Privatsphäre erwartet?

Weitere Kriterien

- Enthält die Verarbeitung andere Auswirkungen, die die Privatsphäre beeinträchtigen können?

## 4.2 Entscheidungsbaum

Die im Abschnitt 4.1 beschriebenen Kriterien sind im nachfolgenden Entscheidungsbaum (siehe Abbildung 2) einfach und kompakt zusammengefasst. Ein einfaches Durchlaufen des Baumes führt zu einer Entscheidung, ob eine DPIA durchzuführen ist.

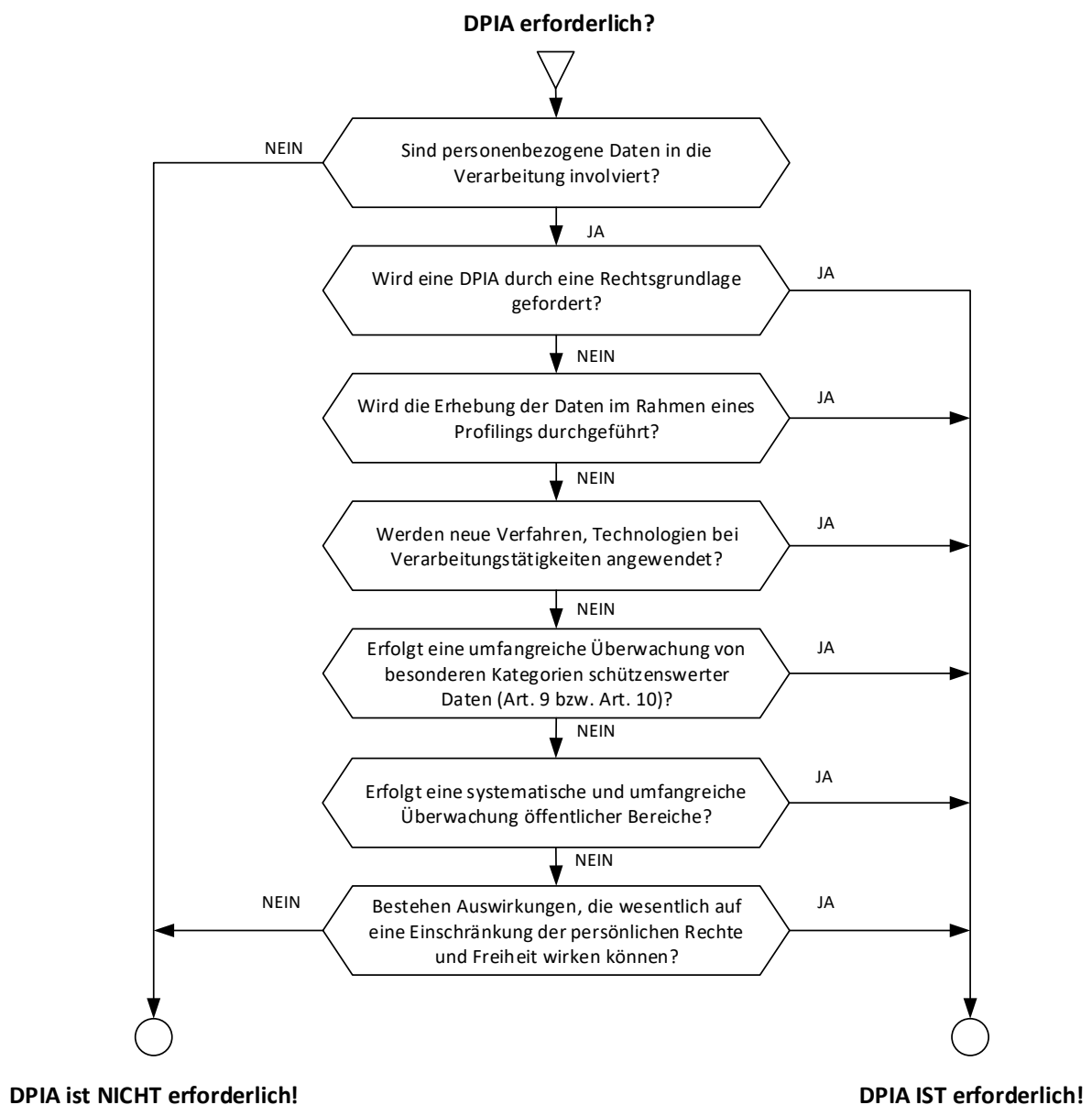


Abbildung 2: Entscheidungsbaum

## 5 Strukturierung eines DPIA-Modells

Abbildung 3 zeigt ein Modell, das hilft die DPIA durchzuführen. An der Wurzel der Betrachtung steht der Betroffene bzw. die Gruppe der Betroffenen. Jene Verarbeitungstätigkeiten, die personenbezogene Daten des Betroffenen für einen klar festgelegten Zweck verarbeiten, werden jeweils darunter angeordnet. In der Beziehung Betroffener zu Verarbeitungstätigkeit wird der jeweilige Grad an Betroffenheit, entsprechend der Tabelle 2, im Rahmen eines Privacy Impact Assessments (PIA) festgestellt. Die Beurteilung erfolgt auf Basis der Kriterien:

1. Verfügbarkeit
2. Vertraulichkeit
3. Integrität
4. Nichtverkettabarkeit
5. Transparenz
6. Intervenierbarkeit

Werden in der PIA Bedrohungen von „HOCH“ oder „SEHR HOCH“ festgestellt, so ist für diese Verarbeitungstätigkeit eine DPIA erforderlich.

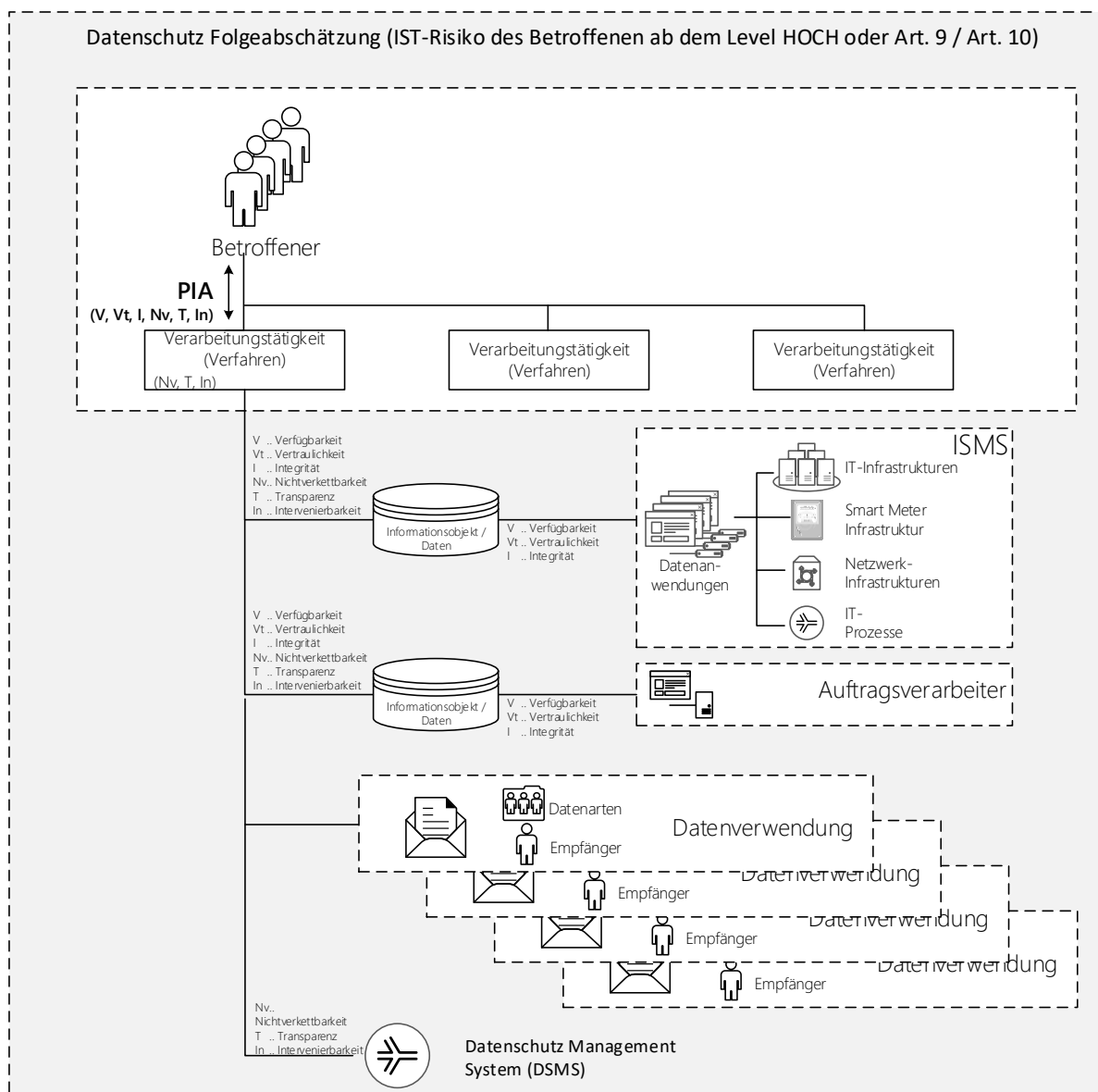


Abbildung 3: Struktur der DPIA Analyse

Jede betrachtete Verarbeitungstätigkeit verarbeitet personenbezogene Daten einer bestimmten Informationskategorie (Informationsobjekt). Die darin gespeicherten Daten werden sowohl von Smart Meter Infrastrukturen, als auch SW-Anwendungen verarbeitet.

Sofern Daten von beauftragten Dritten verarbeitet werden, sind die in der DSGVO festgelegten Richtlinien für Auftragsdatenverarbeiter zugrunde zu legen.

Jede Verarbeitungstätigkeit sieht für die Verarbeitung jeweils mindestens eine Datenverwendung vor, in der einzelne Datenarten als Teil der Informationsobjekte von bestimmten Empfängern der Daten zu festgelegten Zwecken verarbeitet werden.

Über der gesamten Verarbeitung der Daten steht der gesamte Datenschutz Managementprozess der mit seinem Reifegrad zur Reduktion möglicher Folgen (Risiken) für die betroffene natürliche Person beiträgt.

## 6 Berichterstattung

Im DPIA Prozess werden zyklisch entsprechende Analysen betrieben, um den aktuellen Stand der potentiellen Gefahren für die betroffene natürliche Person feststellen zu können. Ein besonderes Augenmerk ist dabei auf die Ausbildung und Betrachtung der Informationssicherheit der IT- und Smart Meter Infrastrukturen zu legen, da der fortschreitende Stand der Technik und die Bedrohungslage durch unberechtigte Dritte einer ständigen Veränderung unterliegen.

Das Ergebnis der DPIA Analyse wird in einem Bericht dargestellt, der sich sowohl aus dem Verzeichnis der Verarbeitungstätigkeiten, als auch aus der Risikoanalyse und der Folgenabschätzung für die betroffene, natürliche Person zusammensetzt.

### Inhaltsverzeichnis

|     |                                                                   |    |
|-----|-------------------------------------------------------------------|----|
| 1   | Präambel.....                                                     | 4  |
| 1.1 | Zielsetzung.....                                                  | 4  |
| 1.2 | Definitionen.....                                                 | 4  |
| 2   | Allgemeine Unternehmensdaten.....                                 | 6  |
| 3   | Erfordernis der Durchführung einer DPIA.....                      | 6  |
| 3.1 | Erklärung der Beurteilungskriterien.....                          | 6  |
| 3.2 | Liste der Verarbeitungstätigkeiten im Smart Metering Prozess..... | 7  |
| 4   | Verzeichnis der DPIA relevanten Verarbeitungstätigkeiten.....     | 8  |
| 5   | Identifikation der relevanten Bedrohungen für Betroffene.....     | 10 |
| 5.1 | Consumer.....                                                     | 10 |
| 5.2 | Prosumer.....                                                     | 10 |
| 6   | Risikobewertung für den Datenschutz.....                          | 12 |
| 6.1 | Consumer.....                                                     | 12 |
| 6.2 | Consumer.....                                                     | 18 |
| 7   | Top 5 Risiken.....                                                | 24 |
| 7.1 | Consumer.....                                                     | 24 |
| 7.2 | Prosumer.....                                                     | 24 |
| 8   | Glossar.....                                                      | 25 |

Abbildung 4: Struktur des DPIA Reports

In der Abbildung 4 ist die Strukturierung bzw. der Inhalt des DPIA Berichtes dargestellt.

## 7 Beurteilung der Bedrohung Betroffener

Die gegenständlich beschriebene DPIA basiert auf einer sehr eingeschränkten Gruppe an betroffenen, natürlichen Personen, deren personenbezogene Daten im Rahmen des Smart Metering Prozesses in den im Abschnitt 2.1 aufgelisteten Verarbeitungstätigkeiten verarbeitet werden. Aufgrund der Einheitlichkeit der Bedrohungslagen kann und sollten nachfolgende vom Arbeitskreis bei Österreichs Energie festgelegten Beurteilungskriterien im Rahmen des Privacy Impact Assessment (PIA) (siehe Tabelle 2) berücksichtigt werden.

### 7.1 Kundeninfo über bevorstehenden SM-Einbau

|                      |                     |             |                                                                             |
|----------------------|---------------------|-------------|-----------------------------------------------------------------------------|
| <b>Beschreibung:</b> |                     |             |                                                                             |
| <b>Beurteilung:</b>  | <b>Kriterium</b>    | <b>Wert</b> | <b>Begründung</b>                                                           |
|                      | Verfügbarkeit       | U           | Keine Auswirkung                                                            |
|                      | Vertraulichkeit     | G           | Keine Art 9, 10 Daten, kein Profiling, nur Kundennummer, Name und Zählpunkt |
|                      | Integrität          | G           | Offenlegung pers. bez. kommen zu einer fremden Person                       |
|                      | Nichtverkettbarkeit | G           | Es können keine kritischen Informationen durch Verkettung erzeugt werden.   |
|                      | Transparenz         | G           |                                                                             |
|                      | Intervenierbarkeit  | G           |                                                                             |

### 7.2 Zählerumstellung auf intelligentes Messgerät (IMS oder IME)

|                      |                           |             |                                                                                                                                                                                                                                                                |
|----------------------|---------------------------|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Beschreibung:</b> | Vorort Zählerinstallation |             |                                                                                                                                                                                                                                                                |
| <b>Beurteilung:</b>  | <b>Kriterium</b>          | <b>Wert</b> | <b>Begründung</b>                                                                                                                                                                                                                                              |
|                      | Verfügbarkeit             | G           | Betroffener hat nur geringe Konsequenzen (hat evt. Umsonst Urlaub genommen)                                                                                                                                                                                    |
|                      | Vertraulichkeit           | G           | Daten aus dem Auftrag stehen dem Monteur zur Verfügung (pers. Umfeld kann dem Monteur transparent werden) Datenverlust von Auftragsdaten fremder Kunden durch den Monteur.                                                                                     |
|                      | Integrität                | G           | Zählerstand wurde nicht oder falsch abgelesen, falscher Zähler wird montiert und falsche Verbrauchswerte werden verrechnet. Kleine Differenzen können übersehen werden. Große Abweichungen werden durch Plausibilitätsprüfungen rasch entdeckt und korrigiert. |
|                      | Nichtverkettbarkeit       | G           | Es können keine kritischen Informationen durch Verkettung erzeugt werden.                                                                                                                                                                                      |
|                      | Transparenz               | G           |                                                                                                                                                                                                                                                                |
|                      | Intervenierbarkeit        | G           |                                                                                                                                                                                                                                                                |

### 7.3 Parametrisierung des DSZ (dig. Standardzähler)

|                      |                     |             |                                                                                                                                      |
|----------------------|---------------------|-------------|--------------------------------------------------------------------------------------------------------------------------------------|
| <b>Beschreibung:</b> |                     |             |                                                                                                                                      |
| <b>Beurteilung:</b>  | <b>Kriterium</b>    | <b>Wert</b> | <b>Begründung</b>                                                                                                                    |
|                      | Verfügbarkeit       | G           | Programmierung wird auf Standard-Setup (1/4 Stundenwerte) bleiben kann aber nicht ausgelesen werden. (nur bei Remote-Parametrierung) |
|                      | Vertraulichkeit     | G           | Keine Verknüpfung mit den Kundendaten vorhanden                                                                                      |
|                      | Integrität          | H           | Opt Out ist ein wichtiger Parameter. Auslesung der ¼ Stundenwerte (Profiling) erfolgt, obwohl nicht erlaubt.                         |
|                      | Nichtverkettbarkeit | G           | Es können keine kritischen Informationen durch Verkettung erzeugt werden.                                                            |

|  |                    |   |  |
|--|--------------------|---|--|
|  | Transparenz        | H |  |
|  | Intervenierbarkeit | H |  |

#### 7.4 Parametrisierung des IMS (Erstmaliges Laden bzw. Änderung eines Parametersatzes)

|                      |                     |             |                                                                                                                                      |
|----------------------|---------------------|-------------|--------------------------------------------------------------------------------------------------------------------------------------|
| <b>Beschreibung:</b> |                     |             |                                                                                                                                      |
| <b>Beurteilung:</b>  | <b>Kriterium</b>    | <b>Wert</b> | <b>Begründung</b>                                                                                                                    |
|                      | Verfügbarkeit       | G           | Programmierung wird auf Standard-Setup (1/4 Stundenwerte) bleiben kann aber nicht ausgelesen werden. (nur bei Remote-Parametrierung) |
|                      | Vertraulichkeit     | G           | Keine Verknüpfung mit den Kundendaten vorhanden                                                                                      |
|                      | Integrität          | H           | Auslesung der ¼ Stundenwerte (Profiling) erfolgt, obwohl nicht erlaubt.                                                              |
|                      | Nichtverkettbarkeit | G           | Es können keine kritischen Informationen durch Verkettung erzeugt werden.                                                            |
|                      | Transparenz         | H           |                                                                                                                                      |
|                      | Intervenierbarkeit  | H           |                                                                                                                                      |

#### 7.5 Parametrisierung des IME (Erstmaliges Laden bzw. Änderung eines Parametersatzes)

|                      |                     |             |                                                                                                                                                                                                    |
|----------------------|---------------------|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Beschreibung:</b> |                     |             |                                                                                                                                                                                                    |
| <b>Beurteilung:</b>  | <b>Kriterium</b>    | <b>Wert</b> | <b>Begründung</b>                                                                                                                                                                                  |
|                      | Verfügbarkeit       | G           | Programmierung wird auf Standard-Setup (1/4 Stundenwerte) bleiben kann aber nicht ausgelesen werden. (nur bei Remote-Parametrierung)                                                               |
|                      | Vertraulichkeit     | G           | Keine Verknüpfung mit den Kundendaten vorhanden                                                                                                                                                    |
|                      | Integrität          | M           | Erfassung der ¼ Stundenwerte (Profiling) ist freigegeben. Maximal werden diese Werte nicht ausgelesen. Werte können evtl. falsch verrechnet werden (falscher Tarif). Korrektur ist schwer möglich. |
|                      | Nichtverkettbarkeit | G           | Es können keine kritischen Informationen durch Verkettung erzeugt werden.                                                                                                                          |
|                      | Transparenz         | M           |                                                                                                                                                                                                    |
|                      | Intervenierbarkeit  | M           |                                                                                                                                                                                                    |

#### 7.6 Ablesung der ¼ Stundenwerte am Zähler am Meterdisplay durch den Kunden oder Vertreter

|                      |                     |             |                                                                                                                                                             |
|----------------------|---------------------|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Beschreibung:</b> |                     |             |                                                                                                                                                             |
| <b>Beurteilung:</b>  | <b>Kriterium</b>    | <b>Wert</b> | <b>Begründung</b>                                                                                                                                           |
|                      | Verfügbarkeit       | G           | Zähler funktioniert dennoch                                                                                                                                 |
|                      | Vertraulichkeit     | H           | Ein Ablesen der gespeicherten Werte ist durch Einwilligung des Betroffenen erst freigeschaltet. Dadurch kann eine unberechtigte Ablesung ermöglicht werden. |
|                      | Integrität          | H           | Das Auslesen am Zähler ist möglich, obwohl nicht erlaubt                                                                                                    |
|                      | Nichtverkettbarkeit | H           | Profiling durch Verknüpfung von Anlage und dem Wissen über den Betroffenen                                                                                  |
|                      | Transparenz         | H           |                                                                                                                                                             |
|                      | Intervenierbarkeit  | H           |                                                                                                                                                             |

## 7.7 Automatisierte Auslesung der DSZ (dig. Standardzähler) entsprechend der ELWOG Vorgaben durch den Netzbetreiber

|                      |                     |             |                                                              |
|----------------------|---------------------|-------------|--------------------------------------------------------------|
| <b>Beschreibung:</b> |                     |             |                                                              |
| <b>Beurteilung:</b>  | <b>Kriterium</b>    | <b>Wert</b> | <b>Begründung</b>                                            |
|                      | Verfügbarkeit       | U           | Ist das Problem des Netzbetreibers und nicht des Betroffenen |
|                      | Vertraulichkeit     | G           | Geringe Auswirkung bei Offenlegung einzelner Verbrauchswerte |
|                      | Integrität          | G           | Wird aufgrund der Plausibilisierung erkannt                  |
|                      | Nichtverkettbarkeit | G           | Es sind nur Einzelwerte                                      |
|                      | Transparenz         | G           |                                                              |
|                      | Intervenierbarkeit  | G           |                                                              |

## 7.8 Automatisierte Auslesung des IMS entsprechend der ELWOG Vorgaben durch den Netzbetreiber

|                      |                     |             |                                                                                                   |
|----------------------|---------------------|-------------|---------------------------------------------------------------------------------------------------|
| <b>Beschreibung:</b> |                     |             |                                                                                                   |
| <b>Beurteilung:</b>  | <b>Kriterium</b>    | <b>Wert</b> | <b>Begründung</b>                                                                                 |
|                      | Verfügbarkeit       | U           | Die Information am Portal steht nicht aktuell zur Verfügung. Unannehmlichkeiten können auftreten. |
|                      | Vertraulichkeit     | G           | Geringe Auswirkung bei Offenlegung einzelner Verbrauchswerte.                                     |
|                      | Integrität          | G           | Wird aufgrund der Plausibilisierung erkannt.                                                      |
|                      | Nichtverkettbarkeit | G           | Es sind nur Einzelwerte.                                                                          |
|                      | Transparenz         | G           |                                                                                                   |
|                      | Intervenierbarkeit  | G           |                                                                                                   |

## 7.9 Automatisierte Auslesung des IME entsprechend der ELWOG Vorgaben durch den Netzbetreiber

|                      |                     |             |                                                                                                                                                          |
|----------------------|---------------------|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Beschreibung:</b> |                     |             |                                                                                                                                                          |
| <b>Beurteilung:</b>  | <b>Kriterium</b>    | <b>Wert</b> | <b>Begründung</b>                                                                                                                                        |
|                      | Verfügbarkeit       | U           | Die Information am Portal steht nicht aktuell zur Verfügung. Unannehmlichkeiten können bei lastabhängigen Tarifen auftreten.                             |
|                      | Vertraulichkeit     | H           | Profiling wird durchgeführt.                                                                                                                             |
|                      | Integrität          | G           | Die Information am Portal steht aktuell nicht korrekt (durch Ersatzwerte) zur Verfügung. Unannehmlichkeiten können bei lastabhängigen Tarifen auftreten. |
|                      | Nichtverkettbarkeit | H           | Profiling wird durchgeführt.                                                                                                                             |
|                      | Transparenz         | H           |                                                                                                                                                          |
|                      | Intervenierbarkeit  | H           |                                                                                                                                                          |

## 7.10 10. Manuelle Auslesung eines elektronischen Messgerätes

|                      |                     |             |                                                                                                   |
|----------------------|---------------------|-------------|---------------------------------------------------------------------------------------------------|
| <b>Beschreibung:</b> |                     |             |                                                                                                   |
| <b>Beurteilung:</b>  | <b>Kriterium</b>    | <b>Wert</b> | <b>Begründung</b>                                                                                 |
|                      | Verfügbarkeit       | U           | Die Information am Portal steht nicht aktuell zur Verfügung. Unannehmlichkeiten können auftreten. |
|                      | Vertraulichkeit     | G           | Geringe Auswirkung bei Offenlegung einzelner Verbrauchswerte.                                     |
|                      | Integrität          | G           | Wird aufgrund der Plausibilisierung erkannt.                                                      |
|                      | Nichtverkettbarkeit | G           | Es sind nur Einzelwerte.                                                                          |
|                      | Transparenz         | G           |                                                                                                   |
|                      | Intervenierbarkeit  | G           |                                                                                                   |

## 7.11 Bereitstellung der Verbrauchsdaten am Kundenportal

|                      |                     |             |                                                                                                                              |
|----------------------|---------------------|-------------|------------------------------------------------------------------------------------------------------------------------------|
| <b>Beschreibung:</b> |                     |             |                                                                                                                              |
| <b>Beurteilung:</b>  | <b>Kriterium</b>    | <b>Wert</b> | <b>Begründung</b>                                                                                                            |
|                      | Verfügbarkeit       | U           | Die Information am Portal steht nicht aktuell zur Verfügung. Unannehmlichkeiten können bei lastabhängigen Tarifen auftreten. |
|                      | Vertraulichkeit     | H           | Profiling wird durchgeführt.                                                                                                 |
|                      | Integrität          | M           | Die Information am Portal steht nicht korrekt zur Verfügung.                                                                 |
|                      | Nichtverkettbarkeit | H           | Profiling wird durchgeführt.                                                                                                 |
|                      | Transparenz         | H           |                                                                                                                              |
|                      | Intervenierbarkeit  | H           |                                                                                                                              |

## 7.12 Kundenanmeldung

|                      |                                                |             |                                                                                                                                                                  |
|----------------------|------------------------------------------------|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Beschreibung:</b> | Neuer Kunde meldet sich beim Netzbetreiber an. |             |                                                                                                                                                                  |
| <b>Beurteilung:</b>  | <b>Kriterium</b>                               | <b>Wert</b> | <b>Begründung</b>                                                                                                                                                |
|                      | Verfügbarkeit                                  | G           | Der Kunde (Consumer) wird nicht freigeschaltet – Unannehmlichkeit für den Kunden, Bei einem Prosumer kann ein überschaubarer wirtschaftlicher Schaden entstehen. |
|                      | Vertraulichkeit                                | H           | Kundenstammdaten, Bankdaten etc. und evtl. Versorgungssicherheit (Gesundheitsdaten, Anlagen) werden mit angegeben.                                               |
|                      | Integrität                                     | H           | Kundenstammdaten, Bankdaten etc. und evtl. Versorgungssicherheit (Gesundheitsdaten, Anlagen) werden mit angegeben.                                               |
|                      | Nichtverkettbarkeit                            | H           | Verknüpfung von schützenswerten Daten zu Betroffenen. Info über bedürftige Personen verkettet mit weiteren schützenswerten Daten.                                |
|                      | Transparenz                                    | H           |                                                                                                                                                                  |
|                      | Intervenierbarkeit                             | H           |                                                                                                                                                                  |

## 7.13 Kundenabmeldung

|                      |  |  |  |
|----------------------|--|--|--|
| <b>Beschreibung:</b> |  |  |  |
|----------------------|--|--|--|

|                     |                     |             |                                                                                 |
|---------------------|---------------------|-------------|---------------------------------------------------------------------------------|
| <b>Beurteilung:</b> | <b>Kriterium</b>    | <b>Wert</b> | <b>Begründung</b>                                                               |
|                     | Verfügbarkeit       | G           | Der Kunde (Consumer) wird nicht abgeschaltet – Unannehmlichkeit für den Kunden. |
|                     | Vertraulichkeit     | G           | Keine oder geringe Auswirkungen für den Kunden                                  |
|                     | Integrität          | S           | Gefahr für andere Betroffene durch Anstoß einer Abschaltung                     |
|                     | Nichtverkettbarkeit | G           | Keine Auswirkung aufgrund einer Verkettung verfügbarer Daten.                   |
|                     | Transparenz         | S           |                                                                                 |
|                     | Intervenierbarkeit  | S           |                                                                                 |

## 7.14 Marktkommunikation Lieferant

|                      |                     |             |                                                                                                     |
|----------------------|---------------------|-------------|-----------------------------------------------------------------------------------------------------|
| <b>Beschreibung:</b> |                     |             |                                                                                                     |
| <b>Beurteilung:</b>  | <b>Kriterium</b>    | <b>Wert</b> | <b>Begründung</b>                                                                                   |
|                      | Verfügbarkeit       | G           | Unannehmlichkeiten für den betroffenen Kunden, geringe wirtschaftliche Auswirkung für den Prosumer. |
|                      | Vertraulichkeit     | H           | Profiling (1/4 Sundenwerte bzw. Kundenverhalten), Austausch von Kundenstammdaten,                   |
|                      | Integrität          | H           | Unberechtigte Abschaltung, Übermittlung falscher Lastprofilaten (Profiling)                         |
|                      | Nichtverkettbarkeit | H           | Rückschlüsse auf Kundeneigenschaft, Zahlungsmoral möglich (Profiling)                               |
|                      | Transparenz         | H           |                                                                                                     |
|                      | Intervenierbarkeit  | H           |                                                                                                     |

## 7.15 Telefonauskunft

|                      |                     |             |                                                                                |
|----------------------|---------------------|-------------|--------------------------------------------------------------------------------|
| <b>Beschreibung:</b> |                     |             |                                                                                |
| <b>Beurteilung:</b>  | <b>Kriterium</b>    | <b>Wert</b> | <b>Begründung</b>                                                              |
|                      | Verfügbarkeit       | U           | Unannehmlichkeit für den Kunden (Consumer und Prosumer)                        |
|                      | Vertraulichkeit     | S           | Z.T. werden besonders schützenswerte Daten erhoben, erhalten und beauskunftet. |
|                      | Integrität          | S           | Z.T. werden besonders schützenswerte Daten erhoben, erhalten und beauskunftet. |
|                      | Nichtverkettbarkeit | S           | Z.T. werden besonders schützenswerte Daten erhoben, erhalten und beauskunftet. |
|                      | Transparenz         | S           |                                                                                |
|                      | Intervenierbarkeit  | S           |                                                                                |

## 7.16 Abschaltung

|                      |                                                        |             |                                                                                                                           |
|----------------------|--------------------------------------------------------|-------------|---------------------------------------------------------------------------------------------------------------------------|
| <b>Beschreibung:</b> | Inkl. Vorverarbeitung und Aufbereitung der Abschaltung |             |                                                                                                                           |
| <b>Beurteilung:</b>  | <b>Kriterium</b>                                       | <b>Wert</b> | <b>Begründung</b>                                                                                                         |
|                      | Verfügbarkeit                                          | G           | Der Kunde (Consumer) wird nicht abgeschaltet – Unannehmlichkeit für den Kunden. Wirtschaftlicher Verlust für den Prosumer |
|                      | Vertraulichkeit                                        | H           | Besonders schützenswerte Daten (Art. 9/10) sind involviert.                                                               |
|                      | Integrität                                             | S           | Gefahr für andere Betroffene mit Versorgungssicherheit durch Anstoß einer Abschaltung                                     |
|                      | Nichtverkettbarkeit                                    | H           | Verkettung des Abschaltgrundes mit den Verbrauchs- und Zahlungsdaten.                                                     |

|  |                    |   |  |
|--|--------------------|---|--|
|  | Transparenz        | S |  |
|  | Intervenierbarkeit | S |  |

### 7.17 Wiederinbetriebnahme nach einer Abschaltung

|                      |                     |             |                                                                                                                                                                  |
|----------------------|---------------------|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Beschreibung:</b> |                     |             |                                                                                                                                                                  |
| <b>Beurteilung:</b>  | <b>Kriterium</b>    | <b>Wert</b> | <b>Begründung</b>                                                                                                                                                |
|                      | Verfügbarkeit       | G           | Der Kunde (Consumer) wird nicht freigeschaltet – Unannehmlichkeit für den Kunden, Bei einem Prosumer kann ein überschaubarer wirtschaftlicher Schaden entstehen. |
|                      | Vertraulichkeit     | G           | Es werden nur Anlagendaten und Kundenstamm aktualisiert.                                                                                                         |
|                      | Integrität          | G           | Unangenehm für den Kunden. Wirtschaftlicher Schaden für den Prosumer                                                                                             |
|                      | Nichtverkettbarkeit | G           | Geringe Auswirkung aufgrund einer Verkettung verfügbarer Daten.                                                                                                  |
|                      | Transparenz         | G           |                                                                                                                                                                  |
|                      | Intervenierbarkeit  | G           |                                                                                                                                                                  |

### 7.18 Anforderung an Prepayment

|                      |                     |             |                                                                                       |
|----------------------|---------------------|-------------|---------------------------------------------------------------------------------------|
| <b>Beschreibung:</b> |                     |             |                                                                                       |
| <b>Beurteilung:</b>  | <b>Kriterium</b>    | <b>Wert</b> | <b>Begründung</b>                                                                     |
|                      | Verfügbarkeit       | U           | Keine Auswirkung für den Kunden                                                       |
|                      | Vertraulichkeit     | U           | Es sind keine personenbezogenen Daten involviert.                                     |
|                      | Integrität          | S           | Gefahr für andere Betroffene mit Versorgungssicherheit durch Anstoß einer Abschaltung |
|                      | Nichtverkettbarkeit | H           | Verkettung des Prepaymentgrundes mit den Verbrauchs- und Zahlungsdaten.               |
|                      | Transparenz         | S           |                                                                                       |
|                      | Intervenierbarkeit  | S           |                                                                                       |

## 7.19 Übersicht der PIA-Bewertungen

| Nr. | Verarbeitungstätigkeit                                                                                                    | Consumer      |                |            |                       |             |                    | Prosumer      |                |            |                       |             |                    |
|-----|---------------------------------------------------------------------------------------------------------------------------|---------------|----------------|------------|-----------------------|-------------|--------------------|---------------|----------------|------------|-----------------------|-------------|--------------------|
|     |                                                                                                                           | Verfügbarkeit | Verräulichkeit | Integrität | Nichtverfälschbarkeit | Transparenz | Intervenierbarkeit | Verfügbarkeit | Verräulichkeit | Integrität | Nichtverfälschbarkeit | Transparenz | Intervenierbarkeit |
| 1   | Kundeninfo über bevorstehenden SM-Einbau                                                                                  | U             | G              | G          | G                     | G           | G                  | U             | G              | G          | G                     | G           | G                  |
| 2   | Zählerumstellung auf intelligentes Messgerät (IMS oder IME) (Arbeitsvorbereitung, Montage und Inbetriebnahme beim Kunden) | G             | G              | G          | G                     | G           | G                  | G             | G              | G          | G                     | G           | G                  |
| 3   | Parametrisierung des DSZ (dig. Standardzähler) (Erstmaliges Laden bzw. Änderung eines Parametersatzes)                    | G             | G              | H          | G                     | H           | H                  |               |                |            |                       |             |                    |
| 4   | Parametrisierung des IMS (Erstmaliges Laden bzw. Änderung eines Parametersatzes)                                          | G             | G              | H          | G                     | H           | H                  |               |                |            |                       |             |                    |
| 5   | Parametrisierung des IME (Erstmaliges Laden bzw. Änderung eines Parametersatzes)                                          | G             | G              | M          | G                     | M           | M                  | G             | G              | M          | G                     | M           | M                  |
| 6   | Auslesung der ¼ Stundenwerte am Zähler am Meterdisplay durch den Kunden oder Vertreter                                    | G             | H              | H          | H                     | H           | H                  | G             | H              | H          | H                     | H           | H                  |
| 7   | Automatisierte Auslesung der DSZ (dig. Standardzähler) entsprechend der ELWOG Vorgaben durch den Netzbetreiber            | U             | G              | G          | G                     | G           | G                  |               |                |            |                       |             |                    |
| 8   | Automatisierte Auslesung des IMS entsprechend der ELWOG Vorgaben durch den Netzbetreiber                                  | U             | G              | G          | G                     | G           | G                  |               |                |            |                       |             |                    |
| 9   | Automatisierte Auslesung des IME entsprechend der ELWOG Vorgaben durch den Netzbetreiber                                  | U             | H              | G          | H                     | H           | H                  | U             | H              | G          | H                     | H           | H                  |
| 10  | Manuelle Auslesung eines elektronischen Messgerätes                                                                       | U             | G              | G          | G                     | G           | G                  | U             | G              | G          | G                     | G           | G                  |
| 11  | Bereitstellung der Verbrauchsdaten am Kundenportal                                                                        | U             | H              | M          | H                     | H           | H                  | U             | H              | M          | H                     | H           | H                  |
| 12  | Kundenanmeldung                                                                                                           | G             | H              | H          | H                     | H           | H                  | G             | H              | H          | H                     | H           | H                  |
| 13  | Kundenabmeldung                                                                                                           | G             | G              | S          | G                     | S           | S                  | G             | G              | S          | G                     | S           | S                  |
| 14  | Marktkommunikation Lieferant                                                                                              | G             | H              | H          | H                     | H           | H                  | G             | H              | H          | H                     | H           | H                  |
| 15  | Telefonauskunft                                                                                                           | U             | S              | S          | S                     | S           | S                  | U             | S              | S          | S                     | S           | S                  |
| 16  | Abschaltung                                                                                                               | G             | H              | S          | H                     | S           | S                  | G             | H              | S          | H                     | H           | H                  |
| 17  | Wiederinbetriebnahme nach einer Abschaltung                                                                               | G             | G              | G          | G                     | G           | G                  | G             | G              | G          | G                     | G           | G                  |
| 18  | Anforderung an Prepayment                                                                                                 | U             | U              | S          | H                     | S           | S                  | U             | U              | S          | H                     | S           | S                  |

U ... unbedeutend

G ... gering

M ... mittel

H ... hoch

S ... sehr hoch

## 8 Glossar

|                                                                  |                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Anonymisieren</b>                                             | Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmbar natürlichen Person zugeordnet werden können.                                                                                  |
| <b>Automatische Verarbeitung</b>                                 | Automatische Verarbeitung ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenbearbeitungsanlagen.                                                                                                                                                                                                                                          |
| <b>Betroffener</b>                                               | Betroffener ist jede bestimmte oder bestimmbar Person, zu der personenbezogene Daten gespeichert sind.                                                                                                                                                                                                                                                                             |
| <b>Datenträger</b>                                               | Datenträger kann jedes Medium sein, das geeignet ist, Daten aufzunehmen. Dies kann sowohl ein Blatt Papier, eine Karteikarte als auch ein elektronisches Medium oder ein Mikrofilm sein. Datenträger ist aber auch eine EDV-Liste, wenn diese Informationen aus einer automatisierten Verarbeitung stammen.                                                                        |
| <b>Dritter</b>                                                   | Dritter ist jede Person oder Stelle außerhalb der verantwortlichen Stelle Dritte sind nicht der Betroffene sowie diejenigen Personen und Stellen, die im Inland, in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen. |
| <b>Empfänger</b>                                                 | Empfänger ist jede Person oder Stelle, die Daten erhält.                                                                                                                                                                                                                                                                                                                           |
| <b>Erheben</b>                                                   | Erheben ist das Beschaffen von Daten über den Betroffenen.                                                                                                                                                                                                                                                                                                                         |
| <b>Integrität</b>                                                | Das Kriterium der Integrität von Daten beschreibt eine Eigenschaft von Daten / Informationen, dass diese ohne Zustimmung des Informations- bzw. Dateneigentümers nicht durch eine unzulässige Verarbeitung verändert oder gelöscht wurden.                                                                                                                                         |
| <b>Intervenierbarkeit</b>                                        | Das Kriterium der Intervenierbarkeit beschreibt eine Eigenschaft von Verarbeitungen personenbezogener Daten, die der betroffenen natürlichen Person die Möglichkeit gibt, die Ausübung der ihm zustehenden Rechte wirksam durchsetzen zu können.                                                                                                                                   |
| <b>Juristische Personen</b>                                      | Juristische Personen sind Kapitalgesellschaften, eingetragene Vereine und Personengesellschaften                                                                                                                                                                                                                                                                                   |
| <b>Löschen</b>                                                   | Löschen ist das Unkenntlich machen gespeicherter personenbezogener Daten.                                                                                                                                                                                                                                                                                                          |
| <b>Mobile personenbezogene Speicher- und Verarbeitungsmedien</b> | Mobile personenbezogene Speicher- und Verarbeitungsmedien sind Datenträger, die an den Betroffenen ausgegeben werden, auf denen personenbezogene Daten über die Speicherung hinaus durch die ausgegebene oder eine andere Stelle automatisiert verarbeitet werden können und bei denen der Betroffene diese Verarbeitung nur durch den Gebrauch des Mediums beeinflussen kann.     |
| <b>Natürliche Personen</b>                                       | Natürliche Personen sind neben Einzelpersonen auch Familien und andere Personengruppen mit einem eigenen „Innenraum (persönlicher Bereich)“, der schutzwürdig ist. Einzelkaufleute - ob im Handelsregister eingetragen oder nicht - werden ebenfalls immer vom Schutz des Gesetzes erfasst.                                                                                        |
| <b>Nicht automatisierte Datei</b>                                | Nicht automatisierte Datei ist jede nicht automatische Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen zugänglich ist und ausgewertet werden kann.                                                                                                                                                                                   |
| <b>Nichtverkettbarkeit</b>                                       | Das Kriterium der Nichtverkettbarkeit beschreibt eine Eigenschaft von Verarbeitungen personenbezogener Daten, diese nicht oder nur mit unverhältnismäßig hohem Aufwand für einen anderen als den ausgewiesenen Zweck durch Verknüpfung (Verkettung) der Dateninhalte erheben, verarbeiten und nutzen zu können.                                                                    |
| <b>Nutzen</b>                                                    | Nutzen ist das Verwenden von Daten, soweit nicht Verarbeiten vorliegt (z.B. Aufruf auf dem Bildschirm)                                                                                                                                                                                                                                                                             |
| <b>personenbezogene Daten</b>                                    | Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbar natürlichen Person (Betroffener), wie z.B. Alter, Anschrift, Vermögen, Kontonummer, Kfz-Kennzeichen, Äußerungen, Überzeugungen).                                                                                                                           |
| <b>Pseudonymisieren</b>                                          | Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.                                                                                                                                                                                  |

|                               |                                                                                                                                                                                                                                                                                                |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Sensitive Daten</b>        | Sensitive Daten sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.                                                                                            |
| <b>Speichern</b>              | Speichern ist das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zweck ihrer weiteren Verarbeitung oder Nutzung.                                                                                                                                       |
| <b>Sperren</b>                | Sperren ist das Kennzeichnen gespeicherter personenbezogener Daten um ihre weitere Verarbeitung oder Nutzung einzuschränken.                                                                                                                                                                   |
| <b>Transparenz</b>            | Das Kriterium der Transparenz beschreibt eine Eigenschaft von Verarbeitungen personenbezogener Daten, die der betroffenen natürlichen Person die Möglichkeit gibt, die Verarbeitung mit zumutbarem Aufwand nachvollziehen und überprüfen zu können.                                            |
| <b>Übermitteln</b>            | Übermitteln ist das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass die Daten an den Dritten weitergegeben werden oder der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abrufen kann. |
| <b>Verändern</b>              | Verändern ist das inhaltliche Umgestalten personenbezogener gespeicherter Daten.                                                                                                                                                                                                               |
| <b>Verantwortliche Stelle</b> | Verantwortliche Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet, nutzt oder dies durch andere im Auftrag vornehmen lässt.                                                                                                                   |
| <b>Verarbeiten</b>            | Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren, Löschen von personenbezogenen Daten.                                                                                                                                                                                           |
| <b>Verfügbarkeit</b>          | Das Kriterium der Verfügbarkeit von Daten ist ein Maß für die Wahrscheinlichkeit, dass bestimmte Daten zu einem bestimmten Zeitpunkt der betroffenen natürlichen Personen zur Verfügung stehen.                                                                                                |
| <b>Vertraulichkeit</b>        | Vertraulichkeit ist die Eigenschaft einer Information, nur einem beschränkten, klar festgelegten Empfängerkreis vorgesehen zu sein. Eine Weitergabe und Veröffentlichung ohne Zustimmung des Informationseigentümers ist nicht zulässig.                                                       |