**2021/1187-001**
Beschlussvorlage
öffentlich

# Abschluss von Konzessionsverträgen für die Bereiche Strom und Gas

| *Organisationseinheit:* | *Beteiligt:* |
|---|---|
| Finanzmanagement | |

| *Beratungsfolge* | *Ö / N* |
|---|---|
| Hauptausschuss (Vorberatung) | N |
| Stadtrat (Entscheidung) | Ö |

## Beschlussentwurf

## Sachverhalt

Bezüglich der Konzessionsverträge Strom und Gas zwischen der Stadt Völklingen und der Stadtwerke Völklingen Netz GmbH als zukünftigem Konzessionsnehmer bestehen derzeit noch Differenzen bezüglich der in § 10 Abs. 10 der Konzessionsvertragsentwürfe enthaltenen Verpflichtung, dass der Konzessionsnehmer die in Lagepläne eingetragenen Versorgungsanlagen auf Wunsch der Stadt in digitalisierter Form in einem Format übergibt, welches von dem GIS-System der Stadt verarbeitet werden kann.

Seitens der Netzgesellschaft wird dies unter Hinweis auf das IT-Sicherheitsgesetz und auf die Zertifizierung der Netzgesellschaft aufgrund von Sicherheitsbedenken abgelehnt. Auf die als Anlage 1 beigefügte Stellungnahme des Rechtsberaters der Netzgesellschaft, die Fa Dornbach, wird verwiesen.

Dem gegenüber kommt der Rechtsberater der Stadt, die Fa. BBH, in Ihrer Stellungnahme zu dem Ergebnis, dass die Zurverfügungstellung der Netzdaten im GIS-Format sehr wohl zulässig ist, wenn bestimmte in einer gesonderten Vereinbarung festzuhaltende Bedingungen erfüllt werden (siehe Anlage 2).

Seitens der Stadt wird daher kein Anlass gesehen, an § 10 Abs. 10 Änderungen vorzunehmen.

## Anlage/n

- Stellungnahme Fa. Dornbach zu § 10 Abs. 10 (öffentlich)
- Stellungnahme Fa. BBH zu § 10 Abs 10 (öffentlich)

Guten Tag Herr Forster,

haben Sie vielen Dank für Ihre Mail vom 11. November an die Netzgesellschaft nebst Ergänzung durch Herrn Groß. Herr Klein hat mir diese zur Beantwortung weitergeleitet.

Was den Umfang der von der Netzgesellschaft der Stadt bereitzustellenden Netzdaten (§ 10 Abs. 10 des Konzessionsvertrages) betrifft, bestehen unsererseits keinerlei Bedenken, der Stadt als Eigentümerin der öffentlichen Wege wie gewünscht eine Liniengraphik nach Versorgungstyp sowie mit einer Leitungsbeschriftung, aus der sich die Art der Versorgungsleitung ergibt, zur Verfügung zu stellen.

Das GIS-System der Gesellschaft bietet die Möglichkeit, diese Daten manuell in pdf-Dateien zu digitalisieren und diese Dateien dann in elektronischer Form der Stadt zur Verfügung stellen. Wenn dies das gemeinsame Verständnis ist, wären wir uns also bereits grundsätzlich einig.

Gleichzeitig bestehen unsererseits weiterhin erhebliche rechtliche Bedenken, georeferenzierte Daten an Dritte - sei es auch die Stadt, an deren Integrität keinerlei Zweifel bestehen - herauszugeben. Hierüber hatten wir in der letzten Besprechung ja bereits ausführlich diskutiert. Wir erläutern dies nachfolgend gerne noch einmal im Detail:

Zunächst ist es so, dass die uns bekannten Musterverträge, die die kommunalen Spitzenverbände mit großen Netzbetreibern ausgehandelt haben, ausdrücklich nicht die Übergabe georeferenzierter Daten beinhalten. Dies ist nicht nur im Saarland so, sondern z.B. auch in Bayern, wo das Muster sogar im Allgemeinen Ministerialblatt veröffentlicht wurde (vgl. AllMBl. 2015 S. 67). Dort lautet die einschlägige Regelung in § 3 Abs. 2 - ebenso wie im Mustervertrag, den der SSGT für die saarländischen Kommunen verhandelt hat - wie folgt:

*„Der Konzessionsnehmer stellt der Gemeinde auf Wunsch kostenfrei einen aktuellen Netzplan sowie bei konkretem Bedarf projektbezogene Bestandspläne mit einer erforderlichen Einweisung zur Verfügung. Der Netzbetreiber ist für neu zu errichtende Elektrizitätsversorgungsanlagen des Elektrizitätsversorgungsnetzes verpflichtet, Aufzeichnungen über deren Art und deren Anschaffungs- und Herstellungskosten abzügl ich empfangener Zuschüsse zu führen.“*

Es ist also keineswegs so, dass die weitergehende Forderung der Stadt nach georeferenzierten Daten des gesamten Stadtgebiets - wie suggeriert - gewissermaßen „bundesweiter Standard“ sei, sondern im Gegenteil wird der Standard zunächst durch die vorliegenden Musterverträge definiert. Dass Abweichungen hiervon möglich sind, wird nicht bestritten, allerdings ist für weitergehende Forderungen zumindest eine tragfähige Begründung erforderlich, die wir bislang nicht kennen. Das allgemeine Eigentümerinteresse wird mit der Formulierung im Mustervertrag uE hinreichend abgedeckt und diese Handhabung entspricht nach unserer Übersicht auch der Praxis der saarländischen Kommunen.

Selbst wenn es entsprechende Gründe gäbe, bilden jedoch die folgenden gesetzlichen Vorgaben und Handlungsempfehlungen diverser Branchenverbände u.a. die Basis für die verpflichtenden und vorhandenen ISMS- und TSM-Zertifizierungen der Netzgesellschaft, so dass deren Einhaltung zwingend zu gewährleisten ist.

1. *Bereitstellung von Metadaten zu INSPIRE-relevanten Geodatensätzen durch Ver- und Entsorgungsunternehmen - Handlungsempfehlung (Dezember 2016); Herausgeber: Arbeitsgemeinschaft von Bund und Ländern sowie Branchenverbände)*

   *„4. Sicherheitsaspekte*

   *Die von der INSPIRE-Richtlinie betroffenen Geodaten von Infrastrukturen von Ver- und Entsorgungsunternehmen haben gegebenenfalls sensiblen Charakter. Als ein Beispiel für sensible Geodaten seien hier Leitungsnetze und deren zugehörige Betriebsmittel genannt. Dies gilt umso mehr, wenn es sich bei den Anlagen der Ver- und Entsorgung um Kritische Infrastrukturen handelt. Die Transparenzziele und -auflagen der INSPIRE-Richtlinie dürfen daher nicht in Widerspruch zu den Zielen und Maßnahmen zum Schutz Kritischer Infrastrukturen stehen. Betreiber Kritischer Infrastrukturen wurden im Juli 2015 mit dem IT-Sicherheitsgesetz zu mehr Sicherheit hinsichtlich ihrer IT verpflichtet.*

   *[…] Im Falle der Zugänglichkeit dieser Geodaten würde die Zielvorgabe des IT-Sicherheitsgesetzes, die Funktionsfähigkeit Kritischer Infrastrukturen zu gewährleisten, konterkariert, weil potenziellen Angreifern der Angriff auf Kritische Infrastrukturen erst ermöglicht würde. Wenn Kritische Infrastrukturen betroffen sind, liegen daher nachteilige Auswirkungen auf bedeutsame Schutzgüter der öffentlichen Sicherheit im Sinne von § 12 Abs. 1 Geodatenzugangsgesetz (GeoZG) und den entsprechenden Landesgesetzen vor.“*

2. *Sicherheitsaspekte und Hinweise für die Betreiber Kritischer Infrastrukturen im Kontext zu gesetzlichen Informationspflichten (noch unveröffentlicht); Herausgeber: UP KRITIS, Themenarbeitskreis Transparenzpflichten)*

   *„2.3.1 Bereitstellung sensibler Infrastrukturdaten*

   *Grundsätzlich muss ein berechtigtes Interesse vorliegen und der Umfang der Informationsbereitstellung auf den eigentlichen Zweck abgestimmt sein. Im Zweifelsfall muss eine Abstimmung über den erforderlichen Informationsbedarf und –tiefe unter Berücksichtigung der Kritikalität der Informationen herbeigeführt werden. Von wenigen Ausnahmen abgesehen, besteht aber kein Anspruch auf eine Bereitstellung von Informationen zur kompletten Infrastruktur […]*

   *2.3.2 Beschränkung der Bereitstellung kritischer Informationen bzw. Bereitstellung generalisierter Informationen*

   *Es wird empfohlen, grundsätzlich die Kritikalität der Informationen zu beurteilen und mögliche Auswirkungen bei einem Missbrauch […] zu bewerten. Sofern Bedenken vorhanden sind, die den Schutz und die Integrität Kritischer Infrastrukturen betreffen, ist eine Bereitstellung von Informationen äußerst sorgsam zu prüfen. Als Alternative bietet sich oft die Veröffentlichung generalisierter Informationen an, wenn dadurch der Schutz der Anlagen und Systeme gewährleistet werden kann.*

   *[…]*

   - *Regelungen des IT-Sicherheitsgesetz*

   *Mit dem seit Juli 2015 gültigen Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) leistet die Bundesregierung einen Beitrag dazu, Infrastrukturen Deutschlands wirkungsvoll vor Angriffen zu schützen. Betreiber von Kritischen Infrastrukturen sind Angriffsziele wie andere Unternehmen auch, besitzen jedoch ein besonders hohes Schadenspotenzial in Bezug auf die Gesellschaft. Insbesondere im Bereich der Kritischen Infrastrukturen (KRITIS) - wie etwa Strom- und*

*Wasserversorgung, Finanzen oder Ernährung - hätte ein Ausfall oder eine Beeinträchtigung der Versorgungsdienstleistungen dramatische Folgen für Wirtschaft, Staat und Gesellschaft in Deutschland. Die Verfügbarkeit und Sicherheit der IT-Systeme spielt somit, speziell im Bereich der Kritischen Infrastrukturen, eine wichtige und zentrale Rolle. Die bereits für Betreiber Kritischer Infrastrukturen geltenden Meldepflichten an das BSI gelten künftig auch für Unternehmen, die von besonderem öffentlichen Interesse sind. Auch nach dem IT-SiG 2.0 sollen keine Daten zu Kritischen Infrastrukturen der Öffentlichkeit zur Verfügung gestellt werden.*

3. Gemäß den technischen Arbeitsblättern zur Erteilung von Netzauskünften S118 (BDEW) und GW 118 (DVGW) sind die Versorgungsunternehmen zudem verpflichtet, insbesondere den Zweck jeder einzelnen Planauskunft zu prüfen und zu dokumentieren, Wer – Warum - Wann – Welche Auskunft erhalten hat.

Eine generalisierte Herausgabe sicherheitsrelevanter, georeferenzierter Daten über Netzpläne hinaus ohne konkreten Anlass wird hierdurch uE ausgeschlossen, die Einhaltung der technischen Arbeitsblätter ist zwingend für den Erhalt der Sicherheits-Zertifizierungen der Netzgesellschaft.

Möglich ist dagegen - und dazu ist die Netzgesellschaft auch jederzeit wie schon in der Vergangenheit bereit – ein Zugriff über die web-Schnittstelle des GIS-Systems als projektbezogene Ergänzung der zu übergebenden digitalisierten Bestandspläne.

Vor diesem Hintergrund bitten wir um Mitteilung, ob die Regelung in § 10 Abs. 10 des Konzessionsvertrages im Sinne einer Übergabe von digitalisierten Netzplänen im pdf-Format nach Versorgungsart mit Leitungsbeschriftung getroffen werden kann.

Bei Rückfragen stehen wir ihnen selbstverständlich jederzeit gerne zur Verfügung.

Mit freundlichen Grüßen

Jochen Hell

DORNBACH GmbH
Rechtsanwaltsgesellschaft

Büro Saarbrücken
Europaallee 5
66113 Saarbrücken
Fon +49 (681) 8 91 97 - 0
Fax +49 (681) 8 91 97 - 17
eMail: jhell@dornbach.de
www.dornbach.de

Sitz der Gesellschaft: Koblenz
Amtsgericht Koblenz HRB 22978
Geschäftsführer: Ralf Wickert, Dr. jur. Alexander Birkhahn, Dr. jur. Jochen Hell, Dr. jur. Julian Engel, Dr. jur. Franz-Peter Gallois, Silvia Simon

**BBH Consulting AG** · Pfeuferstraße 7 · 81373 München
Stadt Völklingen
Herr Groß
Postfach 102040
66310 Völklingen

**Unser Az.: 2764-18**
(Bitte stets angeben.)

München, 26.11.2021

Victor Stocker
T +49 (89) 23 11 64-939
F +49 (89) 23 11 64-999
muenchen@bbh-beratung.de

**BBH Consulting AG**
Pfeuferstraße 7
D-81373 München
www.bbh-beratung.de

Berlin · München · Köln

Sehr geehrter Herr Groß,

in der E-Mail vom 24.11.2021 wurde die BBH Consulting AG aufgefordert eine Einschätzung abzugeben, ob es nach den bestehenden Vorschriften für die Behandlung kritischer Infrastrukturen zulässig sei, Netzpläne in Form von GIS Daten des lokalen Netzbetreiber an die konzessionsgebende Stadt weiterzugeben. Hierbei handelt es sich lediglich um Pläne mit einer jeweiligen Bezeichnung der Leitung, wie beispielsweise Klassifizierung nach Mittelspannung oder Niederspannung. Die Weitergabe vom Netzbetreiber an die Stadt erfolgt derzeit bereits in Form von gedruckten Plänen.

**Grundsätzlich soll die Frage beantwortet werden, ob eine Weitergabe dieser Daten in einem elektronischen und durch die Stadt weiter-verarbeitbaren Format von dem Netzbetreiber an die Stadt, die TSM-Zertifizierung und/oder die Zertifizierung zur Informationssicherheit gem. § 11 Abs. 1 a EnWG des Netzbetreibers gefährdet oder mit einer Zertifizierung nicht vereinbar ist.**

## I. Hintergrund

In § 11 Abs. 1 a Energiewirtschaftsgesetzt ist festgelegt, dass Betreiber von Energieversorgungsnetzen dazu verpflichtet sind, ein zuverlässiges und leistungsfähiges Energieversorgungsnetz diskriminierungsfrei zu betreiben, zu warten und bedarfsgerecht zu optimieren, zu verstärken und auszubauen, soweit es wirtschaftlich zumutbar ist. **Der Betrieb eines sicheren Energieversorgungsnetzes umfasst insbesondere auch einen angemessenen Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die für einen sicheren Netzbetrieb notwendig sind**. Die Regulierungsbehörde erstellt hierzu im Benehmen mit dem Bundesamt für Sicherheit in der

Informationstechnik einen Katalog von Sicherheitsanforderungen und veröffentlicht diesen. Der Katalog der Sicherheitsanforderungen enthält auch Regelungen zur regelmäßigen Überprüfung der Erfüllung der Sicherheitsanforderungen. Ein angemessener Schutz des Betriebs eines Energieversorgungsnetzes liegt vor, wenn dieser Katalog der Sicherheitsanforderungen eingehalten und dies vom Betreiber dokumentiert worden ist.

Die weiterführende Grundlage für die Sicherheitsanforderungen zum Schutz von Telekommunikations- und elektronische Datenverarbeitungssysteme für Betreiber von Energieversorgungsnetzen sind im IT-Sicherheitskatalog gem. § 11 Abs. 1a Energiewirtschaftsgesetz der Bundesnetzagentur geregelt. Dieser enthält den Geltungsbereich der abzusichernden Systeme und Informationen, konkrete Schutzziele sowie Anforderungen an Netzbetreiber, die unter Berücksichtigung der jeweiligen Schutzziele umzusetzen sind. Eine Kernforderung des verbindlichen IT-Sicherheitskatalogs ist die Einführung eines Informationssicherheits-Managementsystems (ISMS) gemäß DIN ISO/IEC 27001 sowie die Zertifizierung durch eine unabhängige hierfür zugelassene Stelle. Die Anforderungen des Sicherheitskatalogs sind unabhängig von der Größe oder der Anzahl der angeschlossenen Kunden von allen Netzbetreibern zu erfüllen, soweit diese über Systeme verfügen, die in den Anwendungsbereich des Sicherheitskatalogs fallen.

Unter Sicherheit wird in Anlehnung an den in § 1 Absatz 1 EnWG definierten Gesetzeszweck einerseits die technische Anlagensicherheit verstanden, andererseits und vor allem aber auch die allgemeine Versorgungssicherheit. Vor dem Hintergrund einer immer stärkeren Durchdringung des Betriebs von Energieversorgungsnetzen mit Informations- und Kommunikationstechnologie und der damit zunehmenden Bedeutung von IT-Sicherheit umfasst das Ziel der Sicherheit nach dem Willen des Gesetzgebers daher nun auch den angemessenen Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die für einen sicheren Netzbetrieb notwendig sind.

Ein angemessener Schutz liegt gemäß § 11 Absatz 1 a EnWG vor, wenn der Katalog der Sicherheitsanforderungen vom Betreiber eines Energieversorgungsnetzes eingehalten wird. Der IT-Sicherheitskatalog stellt insofern einen Mindeststandard dar. Dabei hat der Netzbetreiber insbesondere auch den allgemein anerkannten „Stand der Technik" in Bezug auf die Absicherung der jeweils eingesetzten Systeme zu beachten sowie die allgemeine IKT-Bedrohungslage und die spezifische Bedrohungslage für die eingesetzten Systeme zu berücksichtigen. Dazu sind geeignete, für den jeweiligen Anwendungsbereich formulierte, ggf. branchen- oder sektorspezifische Sicherheitsstandards sowie relevante Empfehlungen, Anwendungsregeln etc. nach jeweils aktuellem Stand heranzuziehen.

Einer dieser sektorspezifischen Sicherheitsstandards stellt die DIN EN ISO/IEC 27019 dar. Diese Norm erweitert die Anforderungen der DIN EN ISO/IEC 27001 um sektorspezifische Sicherheitsanforderungen und ist ebenfalls zwingend zu beachten und Bestandteil der Zertifizierung.

Der Netzbetreiber ist verpflichtet, die Konformität seines ISMS mit den Anforderungen des IT-Sicherheitskatalogs durch ein Zertifikat zu belegen. Die

Bundesnetzagentur hat hierzu gemeinsam mit der Deutschen Akkreditierungsstelle (DAkkS) ein entsprechendes Verfahren auf der Basis von DIN ISO/IEC 27001 erarbeitet. Die Zertifizierung muss durch eine unabhängige und für die Zertifizierung akkreditierte Stelle durchgeführt werden. Gemäß den derzeitigen Bestimmungen erfolgt die Zertifizierung in einem drei Jahreszyklus. Bestehend aus einem Zertifizierungsaudit und jeweils einem Überwachungsaudit in den darauffolgenden Jahren. Somit findet jedes Jahr mind. ein externes Audit beim Netzbetreiber zum Nachweis der Aufrechterhaltung der Informationssicherheit statt.

## II. Einordnung des Sachverhalts

Der verbindliche branchenspezifische Standard DIN EN ISO/IEC 27019 listet unter Punkt *„8.1.1 Inventarisierung der Werte"* einige Werte (Assets) auf, die für Betreiber von Energienetzen in aller Regel eine besonders hohe Sicherheitsrelevanz aufweisen. So findet sich unter Buchstabe a) folgende Beschreibung:

Werte (Assets) im Bereich der Energieversorgung beinhalten viele sektorspezifische Wertetypen, wie z. B.:

a) Informationen: **Netzpläne**, Fahrplan- und Dispatching-Daten, **geographische und georeferenzierte Informationen**, Krisen- und Notfallpläne, Netzwiederaufbaupläne, Schaltantragsdaten, Messwerte- und Messdaten, Zählwerte und Zählerdaten, Meldungen, Betriebsprotokolle, Anwendungsprogrammier- und Parametrierdaten, Messwert- und Meldungsarchive, Langzeit- und Trenddaten usw.;

**Somit ist in der DIN EN ISO/IEC 27019 eindeutig festgelegt, dass „Netzpläne" und „geographische und georeferenzierte Informationen" als sicherheitsrelevante Werte (Assets) zu sehen sind und Gegenstand der Informationssicherheitszertifizierung gem. § 11 Abs. 1a EnWG sind.**

**Somit ergibt sich die Frage, welche konkreten Sicherheitsvorgaben für diese Art von Informationen gelten und ob eine Weitergabe an Dritte kategorisch auszuschließen ist, oder unter welchen Umständen diese zulässig ist.**

Hierzu spezifiziert der IT-Sicherheitskatalog Anforderungen zur Gewährleistung eines angemessenen Schutzes gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die für einen sicheren Netzbetrieb notwendig sind. So besteht dieses Ziel insbesondere in der Auswahl geeigneter, angemessener und dem allgemein anerkannten Stand der Technik entsprechender Maßnahmen zur Realisierung der folgenden Schutzziele:

- die Sicherstellung der Verfügbarkeit der zu schützenden Systeme und Daten
- die Sicherstellung der Integrität der verarbeiteten Informationen und Systeme,

- die Gewährleistung der Vertraulichkeit der mit den betrachteten Systemen verarbeiteten Informationen.

Verfügbarkeit bedeutet, dass die zu schützenden Systeme und Daten auf Verlangen einer berechtigten Einheit zugänglich und nutzbar sind. Integrität bedeutet zum einen die Richtigkeit und Vollständigkeit der verarbeiteten Daten und zum anderen die korrekte Funktionsweise der Systeme. Unter Vertraulichkeit wird der Schutz der Systeme und Daten vor unberechtigtem Zugriff durch Personen oder Prozesse verstanden.

**Die Angemessenheit der durchzuführenden Maßnahmen ist vom individuellen Schutzbedarf des jeweiligen Netzbetreibers abhängig. In die Ermittlung des individuellen Schutzbedarfs sind sowohl Risiken für den eigenen Netzbetrieb als auch Risiken bzgl. der Sicherheit verbundener Energieversorgungsnetze einzubeziehen.**

**Die Verantwortung für die Erfüllung der Schutzziele trägt der Netzbetreiber, auch wenn er sich hierzu Dritter bedient**. Er stellt die Erarbeitung, Kommunikation, Durchführung und Dokumentation der zur Umsetzung der Schutzziele getroffenen Maßnahmen innerhalb der Organisation sicher[1].

Der IT-Sicherheitskatalog gibt also vor, dass der Netzbetreiber basierend auf einer im Vorfeld durchgeführten Risikoeinschätzung, das Sicherheitsniveau seiner Informationswerte (Assets) festlegt und dementsprechend geeignete technische und organisatorische Maßnahmen ergreift, um diese adäquat zu schützen. Ob der Netzbetreiber diese Risikoeinschätzung korrekt durchgeführt hat und anschließend adäquate Sicherheitsvorkehrungen getroffen hat, ist normalweise Gegenstand der jährlichen Überprüfungen durch den Auditor.

Die DIN EN ISO/IEC 27001 zusammen mit der DIN EN ISO/IEC 27002 und EN ISO/IEC 27019 geben hierzu konkrete Vorgaben und nennen Maßnahmenbeispiele, die für die Herstellung eines ausreichenden Schutzniveaus geprüft und sofern anwendbar auch umzusetzen sind.

Für die Weitergabe von (elektronischen) Netzplänen und/oder geographische und georeferenzierte Informationen wären folgende notwendigen Maßnahmen zu nennen:

Die Weitergabe von sicherheitsrelevanten Daten vom Netzbetreiber an die Stadt dürfte nur auf Basis einer (vertraglichen) Vereinbarung erfolgen. In dieser Vereinbarung müssen Art, Anzahl, Sicherheitsanforderungen, Lösch- und Wiederherstellungsregelungen, etc. festgelegt werden. Der Netzbetreiber müsste sich ebenfalls eine Übersicht geben lassen, welche Mitarbeiter der Stadt oder andere Dritte Zugang/Zugriff zu den Daten erhält. Diese Zugangsberechtigungen müssten einer regelmäßigen Kontrolle unterliegen. Zusätzlich müssten Regelungen zum Life-Cycle der betroffenen Daten zwischen den Parteien vereinbart werden.

[1] Vgl. IT-Sicherheitskatalog gemäß § 11 Absatz 1a Energiewirtschaftsgesetz für Betreiber von Energieversorgungsnetzen (August 2018)

Diese aufgeführten Maßnahmen stellen einen Auszug aus den notwendigen Sicherheitsvorkehrungen dar, die ein Betreiber kritischer Infrastrukturen zum Schutz von sicherheitsrelevanten Informationen umzusetzen hat.

## III. Fazit

Auf Grund unserer Expertise im Bereich der Informationssicherheit sowie unserer jahrelangen Erfahrung im Bereich der Einführung, Betrieb, Auditierung und Zertifizierung von Informationssicherheitsmanagementsystemen kommen wir zu der Einschätzung, dass die Weitergabe von GIS Informationen des Netzbetreibers an die Stadt nicht grundsätzlich unvereinbar mit der Sicherheitszertifizierung des Netzbetreibers gem. §11 Abs. 1a EnWG ist. Jedoch fallen die relevanten Daten eindeutig in den gesetzlich vorgegebenen Geltungsbereich des ISMS des Netzbetreibers. Somit hat der Netzbetreiber zu jeder Zeit sicherzustellen, dass diese sicherheitsrelevanten Informationen einem angemessen Schutzniveau unterliegen. Dieses Schutzniveau legt der Netzbetreiber initial gem. der durchgeführten Risikoeinschätzung eigenständig fest, muss jedoch die einschlägigen Vorgaben der DIN EN ISO/IEC 27001, DIN EN ISO/IEC 27002 sowie EN ISO/IEC 27019 beachten und anwenden. Eine zertifizierungsfähige Weitergabe der Daten dürfte somit nur auf Basis einer Vereinbarung erfolgen, die angemessene technische und organisatorische Maßnahmen zum Schutz der Informationen aufweist und dem Netzbetreiber die Möglichkeit bietet, die Einhaltung dieser Maßnahmen fortlaufend zu überwachen.

Mit freundlichen Grüßen

LL.M. Victor Stocker
Senior Consultant
Datenschutzbeauftragter BBH Consulting AG
Lead Auditor 27001
Information Security Officer