



PLT-IT-Sicherheitshinweis

Fremdfirmen - ausschreibungsrelevante Informationen

Teil 1

PLT-IT-Sicherheitshinweis der Münchner Stadtentwässerung

Klassifikation: TLP: WHITE

Dokumentenversion: 1.2
Datum: 21.02.2022
Status: freigegeben
Ersteller: MSE-234, taktisches IT-Sicherheitsmanagement

Inhaltsverzeichnis

1. Grundsätzliches.....	3
1.1 Zielsetzung.....	3
1.2 Gültigkeit.....	3
1.3 Geltungsbereich.....	3
1.4 Definition.....	3
2. Sicherheitsvorgaben.....	3
2.1 Allgemeines.....	4
2.2 IT-Grundschutz-Kompendium.....	4
2.3 Verpflichtungserklärung.....	4
2.4 eingesetzte Systeme.....	4
2.5 Übersicht PLT-IT-Sicherheitspapiere.....	5
3. Anlagen.....	8
3.1 Muster Verpflichtungserklärung.....	8
3.2 Informationen zum Datenschutz.....	8
4. Hinweise zur Dokumentenklassifizierung.....	9
4.1 Was ist das Traffic Light Protokoll?.....	9
4.2 Welche Einstufungen existieren?.....	9

Dokumentenhistorie

Version	Datum Erstellung / Bearbeitung	Erstellt/ überarbeitet Name	Datum Prüfung Freigabe	Freigabe Name	nächstes Review alle 2 Jahre	Änderungsvermerk
1.0	04.06.2020	Mühlenbeck				erster Entwurf
1.1	11.08.2020	Mühlenbeck	20.08.2020	Hübl	20.08.2022	redaktionelle Änderungen, Anlagen Verpflichtungserklärung und Informationen zum Datenschutz als Anlage hinzugefügt, Verpflichtung zur Nutzung betriebseigener Projektierungssysteme
1.2	16.02.2022	Ottinger	21.02.2022	Mühlenbeck	21.02.2024	Anpassung der Dokumente, DRN-Nummern eingefügt

1. Grundsätzliches

1.1 Zielsetzung

Dieser PLT-IT-Sicherheitshinweis fasst die MSE-weit gültigen Vorgaben zur PLT-IT-Sicherheit für Dritte zusammen. Die Vorgaben sind in verschiedenen PLT-IT-Sicherheitspapieren verankert und sind ausnahmslos zu befolgen.

1.2 Gültigkeit

Diese PLT-IT-Sicherheitshinweis tritt nach ihrer Freigabe durch das taktische Sicherheitsmanagement in Kraft. Die Freigabe einer neuen Version dieser PLT-IT-Sicherheitshinweis setzt die Vorgängerversion außer Kraft.

1.3 Geltungsbereich

Dieser PLT-IT-Sicherheitshinweis gilt verbindlich für die Mitarbeiterinnen und Mitarbeiter der Münchner Stadtentwässerung, die im Rahmen ihrer Aufgabe Ausschreibungen durchführen und dabei im PLT-Umfeld tätig sind. Für Dritte, die PLT-IT-Einrichtungen der Münchner Stadtentwässerung nutzen oder im Auftrag der Münchner Stadtentwässerung im PLT-IT-Umfeld tätig sind bzw. handeln, sind auf die Einhaltung der für sie relevanten Aspekte von diesem PLT-IT-Sicherheitshinweis in geeigneter Weise zu verpflichten (siehe Teil 2 – wird bei der Auftragsvergabe übergeben).

1.4 Definition

Die in diesem PLT-IT-Sicherheitshinweis verwendeten Begriffe sind in der PLT-IT-Sicherheitsrichtlinie Glossar definiert.

2. Sicherheitsvorgaben

Die Münchner Stadtentwässerung sind nach dem IT-Sicherheitsgesetz als Betreiber kritischer Infrastrukturen eingestuft.

Kritische Infrastrukturen (KRITIS) sind Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.

Deshalb haben die Münchner Stadtentwässerung für sich und Ihre Auftragnehmer umfangreiche organisatorische und technische Maßnahmen ergriffen, um den Schutz der kritischen Infrastrukturen zu gewährleisten.

2.1 Allgemeines

Um dem IT-Sicherheitsgesetz als Betreiber einer kritischen Infrastruktur genüge zu tun, wurde bei der Münchner Stadtentwässerung eine „allgemeine Konfigurations- und Administrationsstrategie“ festgelegt. Die Festlegung orientiert sich dabei an den vom Bundesamt für Sicherheit in der Informationstechnik (BSI) festgelegten Begriffen „liberal“ und „restriktiv“.

Für die Prozessleittechnik bei der Münchner Stadtentwässerung wurde die Festlegung „restriktiv“ festgelegt. Mit dieser Festlegung sind alle nachfolgenden Erweiterungen bzw. Modernisierungen im Bereich der Prozessleittechnik ausnahmslos nach der restriktiven Methode umzusetzen. Diese restriktive Vorgehensweise schlägt sich in den weiter unten im Dokument aufgeführten PLT-IT-Sicherheitspapieren nieder.

2.2 IT-Grundschutz-Kompodium

Die Münchner Stadtentwässerung orientieren sich an dem jeweils gültigen IT-Grundschutz-Kompodium, dass jährlich durch das BSI im Februar fortgeschrieben wird. Das IT-Grundschutz-Kompodium steht im Internet auf den Seiten des BSI (www.bsi.bund.de) zur Verfügung. Die Fortschreibungen fließen in die jeweiligen PLT-IT-Sicherheitspapiere der Münchner Stadtentwässerung mit ein.

2.3 Verpflichtungserklärung

Im Falle der Auftragserteilung ist von jedem mit dem Projekt betrauten Mitarbeiter die Verpflichtungserklärung (Verpflichtung nach dem Verpflichtungsgesetz vom 2. März 1974 (BGBl. I S. 469), zuletzt geändert durch Gesetz vom 15. August 1974 (BGBl. IS. 1942)) zu unterzeichnen und an den Auftraggeber zurück zu geben (siehe Anlage).

2.4 eingesetzte Systeme

Um neue Systeme in das PLT-Netz einbringen zu können müssen gewisse Randbedingungen eingehalten werden, dabei gilt es grundsätzlich folgendes zu beachten:

- Es werden keine Hardware basierende Rechnersysteme auf Windows oder Linux Basis mehr aufgebaut und integriert.
- Jedes neu hinzukommende System, oder jede neue Applikation ist in die vorhandene Virtualisierungsumgebung zu integrieren.
- Als Betriebssystem stehen Windows Server und Linux Debian zur Verfügung.
- Jedes System/ jede Applikation ist in eine Domäne zu integrieren. Die Zugriffsberechtigungen sind vorgegeben.
- Die Installation einer Applikation hat nur in der Domäne zu erfolgen.
- Jedes System wird mit einem Virens Scanner der Firma Trendmicro ausgestattet.
- Jedes System wird turnusmäßig mit dem Vulnerability Scanner Greenbone auf Schwachstellen untersucht. Auftretende Schwachstellen sind vor einer Erstinbetriebnahme im PLT-Netz zu beseitigen. Während der Mängelanspruchsfrist hat der Auftragnehmer neu auftretende Schwachstellen ebenfalls zu beseitigen.
- Remote-Zugriffe sind grundsätzlich nicht erlaubt. Installationsarbeiten sind vor Ort durchzuführen.

- Vor dem Einbringen eines neuen Netzwerkteilnehmers oder einer neuen Applikation sind dementsprechende Anträge zu stellen. Ohne genehmigten Antrag ist ein Einbau und eine Inbetriebnahme untersagt.
- Als aktive Netzwerkkomponenten werden nur Switches der Firma Hirschmann und Firewalls der Firma Fortinet eingesetzt. Die Switchvorgabe ist auch für Profinet-Netze verbindlich.
- Als Virtualisierungsumgebung wird vSphere und vSphere Horizon der Firma VMware eingesetzt.
- BlackBox Systeme sind grundsätzlich zu vermeiden. Bei Verwendung von BlackBoxen sind alle Kommunikationsschnittstellen offen zu legen. Vor Einbringen in das Netzwerk werden diese Systeme einem aggressiven Vulnerability Scan unterzogen, um die Stabilität des Systems gewährleisten zu können. Sind Schwachstellen erkannt worden, so sind diese durch den Auftragnehmer umgehend zu beseitigen. Vor einer Erstinbetriebnahme im PLT-Netz dürfen keine Schwachstellen vorhanden sein. Die Beseitigung von Schwachstellen durch den Auftragnehmer gilt bis zum Ablauf der Mängelanspruchsfrist.
- Grundsätzlich sind für Projektierungsarbeiten auf den Kläranlagen und im Kanalnetz nur Projektierungswerkzeuge (Notebooks) der Münchner Stadtentwässerung zugelassen. Diese werden durch den Betreiber zur Verfügung gestellt. In Ausnahmefällen können, nach Rücksprache und Freigabe durch den lokalen PLT-IT-Sicherheitsadministrator oder das PLT-IT-Sicherheitsteam, betriebsfremde Projektierungswerkzeuge verwendet werden. Dies ist in geeigneter Weise zu dokumentieren. Diese Anweisung ist auch für nicht direkt am PLT-Netz angebundene Betriebsmittel anzuwenden (Beispiel: Frequenzumformer am Profibus).

2.5 Übersicht PLT-IT-Sicherheitspapiere

Im folgenden sind die wichtigsten PLT-IT-Sicherheitspapiere aufgelistet, die im Auftragsfall dem Auftragnehmer zur Verfügung gestellt werden, falls diese zur Auftragserbringung notwendig sind. Diese Papiere sind zwingend einzuhalten. In Klammern die Dokumentenreferenznummern DRN zur einfachen Suche im ISMS der Prozessleittechnik.

- **PLT-IT-Sicherheitsrichtlinie-IT-Nutzer (234_0003)**

kurze Inhaltszusammenfassung:

Ziel der PLT-IT-Sicherheit der Münchner Stadtentwässerung ist der Schutz der verarbeiteten digitalen Informationen. Als primäre Schutzobjekte haben Informationen unterschiedliche Schutzbedarfe in Bezug auf die V-I-V-A-Kriterien und müssen entsprechend der Schutzbedarfe verarbeitet werden. Um ein angemessenes Sicherheitsniveau in der Münchner Stadtentwässerung zu gewährleisten, müssen alle Mitarbeiterinnen und Mitarbeiter der Münchner Stadtentwässerung, sowie Dritte, die PLT-IT-Systeme nutzen, sich im Rahmen ihrer Verantwortung beteiligen und beteiligt werden.

- **PLT-IT-Sicherheitsrichtlinie-IT-Schaffender (234_0004)**

kurze Inhaltszusammenfassung:

Als PLT-IT-Schaffende gelten Personen, die mit PLT-IT-Aufgaben betraut sind und bei Konzeption, Erstellung und Betrieb von PLT-IT-Services oder PLT-IT-Systemen bei der Münchner Stadtentwässerung mitwirken.

Ziel der PLT-IT-Sicherheit der Münchner Stadtentwässerung ist der Schutz der verarbeiteten digitalen Informationen. Als primäre Schutzobjekte haben Informationen unterschiedliche Schutzbedarfe in Bezug auf die V-I-V-A-Kriterien und müssen entsprechend der Schutzbedarfe verarbeitet werden. Um dies durch eine geeignete PLT-IT-Infrastruktur zu gewährleisten und die PLT-IT-Nutzer bei der Beachtung der PLT-Sicherheitsvorgaben durch technische Lösungen zu unterstützen.

- **PLT-IT-Sicherheitsregel-Passwort (234_0006)**

kurze Inhaltszusammenfassung:

PLT-IT-Systeme der Münchner Stadtentwässerung sind mit passwortbasierten Authentisierungsverfahren geschützt und diese müssen gewisse Vorgaben zu erfüllen.

- **PLT-IT-Sicherheitsrichtlinie-Klassifikation (234_0007)**

kurze Inhaltszusammenfassung:

Alle in der Prozessleittechnik in digitale und analogen Form vorliegenden Informationen sind zu klassifizieren. Unter Klassifizierung wird die Zuordnung der Informationen zu einer Schutzklasse verstanden. Die Klassifizierung wird nach dem Traffic-Light-Protocol (TLP) durchgeführt.

- **PLT-IT-Sicherheitskonzept Upgrade-, Update und Patch Management (234_0012)**

kurze Inhaltszusammenfassung:

Alle in der Prozessleittechnik verfügbaren aktiven Komponenten sind mit Soft- oder Firmware ausgerüstet. Diese Soft- und Firmware gilt es regelmäßig auf Schwachstellen zu überprüfen. Sollten Schwachstellen, oder neue Softwarestände verfügbar sein, so sind diese in geeigneter Art und Weise zu installieren. Die Vorgehensweise wird in diesem Dokument beschrieben.

Neu eingebrachte Systeme, die nicht in diesem Konzept enthalten sind, bedingen eine Fortschreibung. Diese Fortschreibung ist durch den Auftragnehmer zu erbringen.

- **PLT-IT-Sicherheitskonzept-Fremdfirmen (234_0050)**

kurze Inhaltszusammenfassung:

Hier wird der Umgang mit Fremdfirmen in Bezug auf die kritische Infrastruktur geregelt.

- **PLT-IT-Sicherheitsrichtlinie-passiveVernetzung (234_0018)**

kurze Inhaltszusammenfassung:

Diese PLT-IT-Sicherheitsrichtlinie definiert die grundsätzlichen Vorgaben zum Aufbau der passiven Netzwerk-Infrastrukturen in den Münchner Klärwerken und dem Kanalnetz.

- **PLT-IT-Sicherheitsrichtlinie-aktiveKomponenten (234_0019)**

kurze Inhaltszusammenfassung:

Diese PLT-IT-Sicherheitsrichtlinie definiert die grundsätzlichen Vorgaben zum Aufbau der aktiven Netzwerk-Infrastrukturen in den Münchner Klärwerken und dem Kanalnetz.

- **PLT-IT-Sicherheitsregel-Zutritt und zugehörige Formulare (234_0025)**

kurze Inhaltszusammenfassung:

Diese PLT-IT-Sicherheitsregel regelt den Zutritt zu Gebäuden und Räumen

- **PLT-IT-Sicherheitsregel-Zugang und zugehörige Formulare (234_0030)**

kurze Inhaltszusammenfassung:

Diese PLT-IT-Sicherheitsregel regelt den Zugang zu Schränken.

- **PLT-Handbuch-Projektierungsstandards (234_0046)**

kurze Inhaltszusammenfassung:

In diesem Handbuch sind die grundlegenden Projektierungen des Prozessleitsystems PCS 7 bei der Münchner Stadtentwässerung festgelegt.

- **PLT-IT IBN Netzwerkteilnehmer (234_0056)**

kurze Inhaltszusammenfassung:

Vorgehensweise, wie man einen neuen Netzwerkteilnehmer in das PLT-Netz integriert. Diese gilt für Hardware basierende und virtuelle Systeme gleichermaßen.

- **PLT-IT-Sicherheitsregel Netzwerk Patchauftrag (234_0058)**

kurze Inhaltszusammenfassung:

Vorgehensweise, wie man neue Hardware basierende Systeme physikalisch an das PLT-Netzwerk unter Zuhilfenahme der strukturierten Verkabelung anbindet.

- **PLT-IT-Festplattenentsorgung (234_0049)**

kurze Inhaltszusammenfassung:

Dieses Papier regelt die Entsorgung bzw. Rücknahme von Festplatten.

- **PLT-IT-Sicherheitsrichtlinie Freigabe Software (234_0035)**

kurze Inhaltszusammenfassung:

Vorgehensweise, wie neue, noch nicht in der Prozessleittechnik etablierte Software, für die Nutzung in der Prozessleittechnik freizugeben ist.

- **PLT-IT-Vorfallsbehandlung (234_0020)**

kurze Inhaltszusammenfassung:

Dieses Papier regelt die Erfassung und Behandlung von PLT-IT-Sicherheitsvorfällen.

- **PLT-IT-Erfassung Verlustmeldung (234_0055)**

kurze Inhaltszusammenfassung:

Dieses Papier regelt den Verlust von Gerätschaften in der Prozessleittechnik.

- **PLT-IT-Sicherheitshinweis Schutzbedarfsfeststellung (234_0053)**

kurze Inhaltszusammenfassung:

Dieses Papier dient zur einfacheren Einschätzung des Schutzbedarfes von Objekten nach dem VIVA Prinzip.

Hinweis:

Die Auflistung ist nicht als abschließend zu betrachten, da sich die Prozessleittechnik der Münchner Stadtentwässerung ständig weiterentwickelt. Sollten neue Sicherheitspapiere hinzukommen, oder bestehende angepasst werden, so sind diese als verbindlich anzusehen.

Eine Übersicht der Dokumente finden sich in der Dokumentenmatrix. Dokumente mit der Versionsnummer 0.1 sind noch in der Erstellungsphase.

3. Anlagen

3.1 Muster Verpflichtungserklärung

Muster zur Niederschrift und Erklärung über die Verpflichtung nach § 1 des Verpflichtungsgesetzes.

3.2 Informationen zum Datenschutz

Hier finden Sie Hinweise zum Datenschutz.

4. Hinweise zur Dokumentenklassifizierung

Bitte wenden Sie sich bei allen Rückfragen zu diesem Dokument an denjenigen Kontakt, der Ihnen das Dokument zugesendet hat. Dadurch bleibt der Informationsfluss kanalisiert.

4.1 Was ist das Traffic Light Protokoll?

Das TLP ist ein von der OECD entworfenes Protokoll, welches die Weitergabe von sensiblen Informationen innerhalb eines Informationsverbundes regelt. Die vom Autor adressierten Empfänger dieses Dokumentes haben sich im Vorfeld schriftlich verpflichtet das TLP zu beachten und das Dokument entsprechend den „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten.

4.2 Welche Einstufungen existieren?

TLP:WHITE: Unbegrenzte Weitergabe

Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:WHITE ohne Einschränkungen frei weitergegeben werden.

TLP:GREEN: Organisationsübergreifende Weitergabe

Informationen dieser Stufe dürfen innerhalb der Organisationen und an deren Partner frei weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden.

TLP:AMBER: Eingeschränkte interne und organisationsübergreifende Verteilung

Informationen dieser Stufe darf der Empfänger innerhalb seiner Organisation auf Basis „Kenntnis nur wenn nötig“ weitergeben. Der Empfänger darf die Informationen zudem an Dritte weitergeben, soweit diese die Informationen zum Schutz des Empfängers oder zur Schadensreduktion beim Empfänger benötigen. Hierfür muss er sicherstellen, dass die „Dritten“ das TLP kennen und die damit verbundenen Regeln einhalten. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.

TLP:RED: Persönlich, nur für benannte Empfänger

Informationen dieser Stufe sind auf den Kreis der Anwesenden in einer Besprechung oder Video-/Audiokonferenz bzw. auf die direkten Empfänger bei schriftlicher Korrespondenz beschränkt. Eine Weitergabe ist untersagt. Meistens werden TLP:RED-Informationen mündlich oder persönlich übergeben.

Projekt/ Maßnahme:	Auftrag vom:
Leistung:	Vergabe-Nr.:

Niederschrift und Erklärung über die Verpflichtung

nach § 1 des Verpflichtungsgesetzes vom 02. März 1974 (BGBl. S. 547)
zuletzt geändert durch das Gesetz vom 15. August 1974 (BGBl. I S. 1942)

Frau / Herr

Beschäftigte/r der Firma

ist heute vom Unterzeichnenden auf die gewissenhafte Erfüllung ihrer/seiner Obliegenheiten verpflichtet und auf die strafrechtlichen Folgen einer Pflichtverletzung hingewiesen worden.

Ihr/Ihm wurde der Inhalt der nachfolgend aufgeführten und als Anlage beigefügten Strafvorschriften des Strafgesetzbuches eröffnet:

- § 133 Verwahrungsbruch
- § 201 Verletzung des Vertraulichkeit des Wortes
- § 203 Verletzung von Privatgeheimnissen
- § 204 Verwertung fremder Geheimnisse
- § 331 Vorteilsannahme
- § 332 Bestechlichkeit
- § 333 Vorteilsgewährung
- § 334 Bestechung
- § 335 Besonders schwere Fälle der Bestechlichkeit und Bestechung
- § 353 b Verletzung des Dienstgeheimnisses und einer besonderen Geheimhaltungspflicht
- § 358 Nebenfolgen

Ort, Datum

Dienststelle

Unterschrift der/des Verpflichteten

Unterschrift der/des Verpflichtenden

Anlage: Auszug aus dem Verpflichtungsgesetz und dem Strafgesetzbuch

Verpflichtung nach dem Verpflichtungsgesetz

- Auszug aus den maßgebenden Gesetzesbestimmungen -

1. Auszug aus dem Verpflichtungsgesetz

§ 1

- (1) Auf die gewissenhafte Erfüllung seiner Obliegenheiten soll verpflichtet werden, wer, ohne Amtsträger (§ 11 Abs.1 Nr. 2 des Strafgesetzbuches) zu sein,
1. bei einer Behörde oder bei einer sonstigen Stelle, die Aufgaben der öffentlichen Verwaltung wahrnimmt, beschäftigt oder für sie tätig ist,
 2. bei einem Verband oder sonstigen Zusammenschluss, einem Betrieb oder Unternehmen, die für eine Behörde oder sonstige Stelle Aufgaben der öffentlichen Verwaltung ausführen, beschäftigt oder für sie tätig ist oder
 3. als Sachverständiger öffentlich bestellt ist.
- (2) Die Verpflichtung wird mündlich vorgenommen. Dabei ist auf die strafrechtlichen Folgen einer Pflichtverletzung hinzuweisen.
- (3) Über die Verpflichtung wird eine Niederschrift aufgenommen, die der Verpflichtete mit unterzeichnet. Er erhält eine Abschrift der Niederschrift; davon kann abgesehen werden, wenn dies im Interesse der inneren oder äußeren Sicherheit der Bundesrepublik Deutschland geboten ist.
- (4) Welche Stelle für die Verpflichtung zuständig ist, bestimmt
1. in den Fällen des Absatzes 1 Nr. 1 und 2 bei Behörden oder sonstigen Stellen nach Bundesrecht die jeweils zuständige oberste Dienstaufsichtsbehörde oder, soweit eine Dienstaufsicht nicht besteht, die oberste Fachaufsichtsbehörde.
 2. in allen übrigen Fällen diejenige Behörde, die von der Landesregierung durch Rechtsverordnung bestimmt wird.

2. Auszug aus dem Strafgesetzbuch

§ 11 Personen und Sachbegriffe

- (1) Im Sinne dieses Gesetzes ist
- ...
2. Amtsträger:
wer nach deutschem Recht
- a) Beamter oder Richter ist,
 - b) in einem sonstigen öffentlich-rechtlichen Amtsverhältnis steht oder
 - c) sonst dazu bestellt ist, bei einer Behörde oder bei einer sonstigen Stelle oder in deren Auftrag Aufgaben der öffentlichen Verwaltung unbeschadet der zur Aufgabenerfüllung gewählten Organisationsform wahrzunehmen;
- ...
4. für den öffentlichen Dienst besonders Verpflichteter:
wer, ohne Amtsträger zu sein,
- a) bei einer Behörde oder bei einer sonstigen Stelle, die Aufgaben der öffentlichen Verwaltung wahrnimmt, oder
 - b) bei einem Verband oder sonstigen Zusammenschluss, Betrieb oder Unternehmen, die für eine Behörde oder für eine sonstige Stelle Aufgaben der öffentlichen Verwaltung ausführen, beschäftigt oder für sie tätig und auf die gewissenhafte Erfüllung seiner Obliegenheiten auf Grund eines Gesetzes förmlich verpflichtet ist.

§ 133 Verwahrungsbruch

(1) Wer Schriftstücke oder andere bewegliche Sachen, die sich in dienstlicher Verwahrung befinden oder ihm oder einem anderen dienstlich in Verwahrung gegeben worden sind, zerstört, beschädigt, unbrauchbar macht oder der dienstlichen Verfügung entzieht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) Dasselbe gilt für Schriftstücke oder andere bewegliche Sachen, die sich in amtlicher Verwahrung einer Kirche oder anderen Religionsgesellschaft des öffentlichen Rechts befinden oder von dieser dem Täter oder einem anderen amtlich in Verwahrung gegeben worden sind.

(3) Wer die Tat an einer Sache begeht, die ihm als Amtsträger oder für den öffentlichen Dienst besonders Verpflichteten anvertraut worden oder zugänglich geworden ist, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

§ 201 Verletzung der Vertraulichkeit des Wortes

(1) Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer unbefugt

1. das nichtöffentlich gesprochene Wort eines anderen auf einen Tonträger aufnimmt oder
2. eine so hergestellte Aufnahme gebraucht oder einem Dritten zugänglich macht.

(2) Ebenso wird bestraft, wer unbefugt

1. das nicht zu seiner Kenntnis bestimmte nichtöffentlich gesprochene Wort eines anderen mit einem Abhörgerät abhört oder
2. das nach Absatz 1 Nr. 1 aufgenommene oder nach Absatz 2 Nr. 1 abgehörte nichtöffentlich gesprochene Wort eines anderen im Wortlaut oder seinem wesentlichen Inhalt nach öffentlich mitteilt. Die Tat nach Satz 1 Nr. 2 ist nur strafbar, wenn die öffentliche Mitteilung geeignet ist, berechnete Interessen eines anderen zu beeinträchtigen. Sie ist nicht rechtswidrig, wenn die öffentliche Mitteilung zur Wahrnehmung überragender öffentlicher Interessen gemacht wird.

(3) Mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe wird bestraft, wer als Amtsträger oder als für den öffentlichen Dienst besonders Verpflichteter die Vertraulichkeit des Wortes verletzt (Absätze 1 und 2).

(4) Der Versuch ist strafbar.

(5) Die Tonträger und Abhörgeräte, die der Täter oder Teilnehmer verwendet hat, können eingezogen werden. § 74a ist anzuwenden.

§ 203 Verletzung von Privatgeheimnissen

(1) Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als

1. Arzt, Zahnarzt, Tierarzt, Apotheker oder Angehörigen eines anderen Heilberufs, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert,

2. Berufspsychologen mit staatlich anerkannter wissenschaftlicher Abschlußprüfung,

3. Rechtsanwalt, Patentanwalt, Notar, Verteidiger in einem gesetzlich geordneten Verfahren, Wirtschaftsprüfer, vereidigter Buchprüfer, Steuerberater, Steuerbevollmächtigter oder Organ oder Mitglied eines Organs einer Rechtsanwalts-, Patentanwalts-, Wirtschaftsprüfungs-, Buchprüfungs- oder Steuerberatungsgesellschaft,

4. Ehe-, Familien-, Erziehungs- oder Jugendberater sowie Berater für Suchtfragen in einer Beratungsstelle, die von einer Behörde oder Körperschaft, Anstalt oder Stiftung des öffentlichen Rechts anerkannt ist,

4a. Mitglied oder Beauftragter einer anerkannten Beratungsstelle nach den §§ 3 und 8 des Schwangerschaftskonfliktgesetzes,

5. staatlich anerkanntem Sozialarbeiter oder staatlich anerkanntem Sozialpädagogen oder

6. Angehörigen eines Unternehmens der privaten Kranken-, Unfall- oder Lebensversicherung oder einer privatärztlichen, steuerberaterlichen oder anwaltlichen Verrechnungsstelle

anvertraut worden oder sonst bekanntgeworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als

1. Amtsträger,

2. für den öffentlichen Dienst besonders Verpflichteten,

3. Person, die Aufgaben oder Befugnisse nach dem Personalvertretungsrecht wahrnimmt,

4. Mitglied eines für ein Gesetzgebungsorgan des Bundes oder eines Landes tätigen Untersuchungsausschusses, sonstigen Ausschusses oder Rates, das nicht selbst Mitglied des Gesetzgebungsorgans ist, oder als Hilfskraft eines solchen Ausschusses oder Rates,
5. öffentlich bestelltem Sachverständigen, der auf die gewissenhafte Erfüllung seiner Obliegenheiten auf Grund eines Gesetzes förmlich verpflichtet worden ist, oder
6. Person, die auf die gewissenhafte Erfüllung ihrer Geheimhaltungspflicht bei der Durchführung wissenschaftlicher Forschungsvorhaben auf Grund eines Gesetzes förmlich verpflichtet worden ist, anvertraut worden oder sonst bekanntgeworden ist. Einem Geheimnis im Sinne des Satzes 1 stehen Einzelangaben über persönliche oder sachliche Verhältnisse eines anderen gleich, die für Aufgaben der öffentlichen Verwaltung erfaßt worden sind; Satz 1 ist jedoch nicht anzuwenden, soweit solche Einzelangaben anderen Behörden oder sonstigen Stellen für Aufgaben der öffentlichen Verwaltung bekanntgegeben werden und das Gesetz dies nicht untersagt.
- (3) Kein Offenbaren im Sinne dieser Vorschrift liegt vor, wenn die in den Absätzen 1 und 2 genannten Personen Geheimnisse den bei ihnen berufsmäßig tätigen Gehilfen oder den bei ihnen zur Vorbereitung auf den Beruf tätigen Personen zugänglich machen. Die in den Absätzen 1 und 2 Genannten dürfen fremde Geheimnisse gegenüber sonstigen Personen offenbaren, die an ihrer beruflichen oder dienstlichen Tätigkeit mitwirken, soweit dies für die Inanspruchnahme der Tätigkeit der sonstigen mitwirkenden Personen erforderlich ist; das Gleiche gilt für sonstige mitwirkende Personen, wenn diese sich weiterer Personen bedienen, die an der beruflichen oder dienstlichen Tätigkeit der in den Absätzen 1 und 2 Genannten mitwirken.
- (4) Mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe wird bestraft, wer unbefugt ein fremdes Geheimnis offenbart, das ihm bei der Ausübung oder bei Gelegenheit seiner Tätigkeit als mitwirkende Person oder als bei den in den Absätzen 1 und 2 genannten Personen tätiger Beauftragter für den Datenschutz bekannt geworden ist. Ebenso wird bestraft, wer
1. als in den Absätzen 1 und 2 genannte Person nicht dafür Sorge getragen hat, dass eine sonstige mitwirkende Person, die unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, zur Geheimhaltung verpflichtet wurde; dies gilt nicht für sonstige mitwirkende Personen, die selbst eine in den Absätzen 1 oder 2 genannte Person sind,
2. als im Absatz 3 genannte mitwirkende Person sich einer weiteren mitwirkenden Person, die unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, bedient und nicht dafür Sorge getragen hat, dass diese zur Geheimhaltung verpflichtet wurde; dies gilt nicht für sonstige mitwirkende Personen, die selbst eine in den Absätzen 1 oder 2 genannte Person sind, oder
3. nach dem Tod der nach Satz 1 oder nach den Absätzen 1 oder 2 verpflichteten Person ein fremdes Geheimnis unbefugt offenbart, das er von dem Verstorbenen erfahren oder aus dessen Nachlass erlangt hat.
- (5) Die Absätze 1 bis 4 sind auch anzuwenden, wenn der Täter das fremde Geheimnis nach dem Tod des Betroffenen unbefugt offenbart.
- (6) Handelt der Täter gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, so ist die Strafe Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe.

§ 204 Verwertung fremder Geheimnisse

- (1) Wer unbefugt ein fremdes Geheimnis, namentlich ein Betriebs- oder Geschäftsgeheimnis, zu dessen Geheimhaltung er nach § 203 verpflichtet ist, verwertet, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.
- (2) § 203 Abs. 5 gilt entsprechend.

§ 331 Vorteilsannahme

- (1) Ein Amtsträger, ein Europäischer Amtsträger oder ein für den öffentlichen Dienst besonders Verpflichteter, der für die Dienstaussübung einen Vorteil für sich oder einen Dritten fordert, sich versprechen läßt oder annimmt, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.
- (2) Ein Richter, Mitglied eines Gerichts der Europäischen Union oder Schiedsrichter, der einen Vorteil für sich oder einen Dritten als Gegenleistung dafür fordert, sich versprechen läßt oder annimmt, daß er eine richterliche Handlung vorgenommen hat oder künftig vornehme, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft. Der Versuch ist strafbar.
- (3) Die Tat ist nicht nach Absatz 1 strafbar, wenn der Täter einen nicht von ihm geforderten Vorteil sich versprechen läßt oder annimmt und die zuständige Behörde im Rahmen ihrer Befugnisse entweder die Annahme vorher genehmigt hat oder der Täter unverzüglich bei ihr Anzeige erstattet und sie die Annahme genehmigt.

§ 332 Bestechlichkeit

(1) Ein Amtsträger, ein Europäischer Amtsträger oder ein für den öffentlichen Dienst besonders Verpflichteter, der einen Vorteil für sich oder einen Dritten als Gegenleistung dafür fordert, sich versprechen läßt oder annimmt, daß er eine Diensthandlung vorgenommen hat oder künftig vornehmen und dadurch seine Dienstpflichten verletzt hat oder verletzen würde, wird mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren bestraft. In minder schweren Fällen ist die Strafe Freiheitsstrafe bis zu drei Jahren oder Geldstrafe. Der Versuch ist strafbar.

(2) Ein Richter, Mitglied eines Gerichts der Europäischen Union oder Schiedsrichter, der einen Vorteil für sich oder einen Dritten als Gegenleistung dafür fordert, sich versprechen läßt oder annimmt, daß er eine richterliche Handlung vorgenommen hat oder künftig vornehmen und dadurch seine richterlichen Pflichten verletzt hat oder verletzen würde, wird mit Freiheitsstrafe von einem Jahr bis zu zehn Jahren bestraft. In minder schweren Fällen ist die Strafe Freiheitsstrafe von sechs Monaten bis zu fünf Jahren.

(3) Falls der Täter den Vorteil als Gegenleistung für eine künftige Handlung fordert, sich versprechen läßt oder annimmt, so sind die Absätze 1 und 2 schon dann anzuwenden, wenn er sich dem anderen gegenüber bereit gezeigt hat,

1. bei der Handlung seine Pflichten zu verletzen oder,
2. soweit die Handlung in seinem Ermessen steht, sich bei Ausübung des Ermessens durch den Vorteil beeinflussen zu lassen.

§ 333 Vorteilsgewährung

(1) Wer einem Amtsträger, einem Europäischen Amtsträger, einem für den öffentlichen Dienst besonders Verpflichteten oder einem Soldaten der Bundeswehr für die Dienstaussübung einen Vorteil für diesen oder einen Dritten anbietet, verspricht oder gewährt, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Wer einem Richter, Mitglied eines Gerichts der Europäischen Union oder Schiedsrichter einen Vorteil für diesen oder einen Dritten als Gegenleistung dafür anbietet, verspricht oder gewährt, daß er eine richterliche Handlung vorgenommen hat oder künftig vornehmen, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(3) Die Tat ist nicht nach Absatz 1 strafbar, wenn die zuständige Behörde im Rahmen ihrer Befugnisse entweder die Annahme des Vorteils durch den Empfänger vorher genehmigt hat oder sie auf unverzügliche Anzeige des Empfängers genehmigt.

§ 334 Bestechung

(1) Wer einem Amtsträger, einem Europäischen Amtsträger, einem für den öffentlichen Dienst besonders Verpflichteten oder einem Soldaten der Bundeswehr einen Vorteil für diesen oder einen Dritten als Gegenleistung dafür anbietet, verspricht oder gewährt, daß er eine Diensthandlung vorgenommen hat oder künftig vornehmen und dadurch seine Dienstpflichten verletzt hat oder verletzen würde, wird mit Freiheitsstrafe von drei Monaten bis zu fünf Jahren bestraft. In minder schweren Fällen ist die Strafe Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe.

(2) Wer einem Richter, Mitglied eines Gerichts der Europäischen Union oder Schiedsrichter einen Vorteil für diesen oder einen Dritten als Gegenleistung dafür anbietet, verspricht oder gewährt, daß er eine richterliche Handlung

1. vorgenommen und dadurch seine richterlichen Pflichten verletzt hat oder
 2. künftig vornehmen und dadurch seine richterlichen Pflichten verletzen würde,
- wird in den Fällen der Nummer 1 mit Freiheitsstrafe von drei Monaten bis zu fünf Jahren, in den Fällen der Nummer 2 mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren bestraft. Der Versuch ist strafbar.

(3) Falls der Täter den Vorteil als Gegenleistung für eine künftige Handlung anbietet, verspricht oder gewährt, so sind die Absätze 1 und 2 schon dann anzuwenden, wenn er den anderen zu bestimmen versucht, daß dieser

1. bei der Handlung seine Pflichten verletzt oder,
2. soweit die Handlung in seinem Ermessen steht, sich bei der Ausübung des Ermessens durch den Vorteil beeinflussen läßt.

§ 335 Besonders schwere Fälle der Bestechlichkeit und Bestechung

(1) In besonders schweren Fällen wird

1. eine Tat nach

a) § 332 Abs. 1 Satz 1, auch in Verbindung mit Abs. 3, und

b) § 334 Abs. 1 Satz 1 und Abs. 2, jeweils auch in Verbindung mit Abs. 3, mit Freiheitsstrafe von einem Jahr bis zu zehn Jahren und

2. eine Tat nach § 332 Abs. 2, auch in Verbindung mit Abs. 3, mit Freiheitsstrafe nicht unter zwei Jahren

bestraft.

(2) Ein besonders schwerer Fall im Sinne des Absatzes 1 liegt in der Regel vor, wenn

1. die Tat sich auf einen Vorteil großen Ausmaßes bezieht,

2. der Täter fortgesetzt Vorteile annimmt, die er als Gegenleistung dafür gefordert hat, daß er eine Diensthandlung künftig vornehme, oder

3. der Täter gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung solcher Taten verbunden hat.

§ 353 b Verletzung des Dienstgeheimnisses und einer besonderen Geheimhaltungspflicht

(1) Wer ein Geheimnis, das ihm als

1. Amtsträger,

2. für den öffentlichen Dienst besonders Verpflichteten oder

3. Person, die Aufgaben oder Befugnisse nach dem Personalvertretungsrecht wahrnimmt, anvertraut worden oder sonst bekanntgeworden ist, unbefugt offenbart und dadurch wichtige öffentliche Interessen gefährdet, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft. Hat der Täter durch die Tat fahrlässig wichtige öffentliche Interessen gefährdet, so wird er mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2) Wer, abgesehen von den Fällen des Absatzes 1, unbefugt einen Gegenstand oder eine Nachricht, zu deren Geheimhaltung er

1. auf Grund des Beschlusses eines Gesetzgebungsorgans des Bundes oder eines Landes oder eines seiner Ausschüsse verpflichtet ist oder

2. von einer anderen amtlichen Stelle unter Hinweis auf die Strafbarkeit der Verletzung der Geheimhaltungspflicht förmlich verpflichtet worden ist,

an einen anderen gelangen läßt oder öffentlich bekanntmacht und dadurch wichtige öffentliche Interessen gefährdet, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(3) Der Versuch ist strafbar.

(3a) Beihilfehandlungen einer in § 53 Absatz 1 Satz 1 Nummer 5 der Strafprozessordnung genannten Person sind nicht rechtswidrig, wenn sie sich auf die Entgegennahme, Auswertung oder Veröffentlichung des Geheimnisses oder des Gegenstandes oder der Nachricht, zu deren Geheimhaltung eine besondere Verpflichtung besteht, beschränken.

(4) Die Tat wird nur mit Ermächtigung verfolgt. Die Ermächtigung wird erteilt

1. von dem Präsidenten des Gesetzgebungsorgans

a) in den Fällen des Absatzes 1, wenn dem Täter das Geheimnis während seiner Tätigkeit bei einem oder für ein Gesetzgebungsorgan des Bundes oder eines Landes bekanntgeworden ist,

b) in den Fällen des Absatzes 2 Nr. 1;

2. von der obersten Bundesbehörde

a) in den Fällen des Absatzes 1, wenn dem Täter das Geheimnis während seiner Tätigkeit sonst bei einer oder für eine Behörde oder bei einer anderen amtlichen Stelle des Bundes oder für eine solche Stelle bekanntgeworden ist,

b) in den Fällen des Absatzes 2 Nr. 2, wenn der Täter von einer amtlichen Stelle des Bundes verpflichtet worden ist;

3. von der obersten Landesbehörde in allen übrigen Fällen der Absätze 1 und 2 Nr. 2.

§ 358 Nebenfolgen

Neben einer Freiheitsstrafe von mindestens sechs Monaten wegen einer Straftat nach den §§ 332, 335, 339, 340, 343, 344, 345 Abs. 1 und 3, §§ 348, 352 bis 353 b Abs. 1, §§ 355 und 357 kann das Gericht die Fähigkeit, öffentliche Ämter zu bekleiden (§ 45 Abs. 2), aberkennen.

Anmerkung:

Die vorgenannten Paragraphen sind in der jeweiligen aktuellen Fassung gültig.

**Informationen zum Datenschutz aufgrund Art. 13 Datenschutz-Grundverordnung (DSGVO)
im Zusammenhang mit der Abwicklung von Aufträgen in der Prozessleittechnik und/oder
Nutzung von Prozessdaten der Klärwerke und des Kanalnetzes**

- **Kontaktdaten des Verantwortlichen**

Verantwortlich für die Verarbeitung ist die
Münchner Stadtentwässerung
MSE-234
Friedenstr. 40
81671 München
plt-it-sicherheit.mse@muenchen.de

- **Kontaktdaten des Datenschutzbeauftragten**

Datenschutzbeauftragter der MSE
Friedenstr. 40
81671 München
dsb.mse@muenchen.de

- **Zwecke und Rechtsgrundlagen der Datenverarbeitung**

Wir verarbeiten Ihre personenbezogenen Daten, soweit dies zur Abwicklung von Aufträgen in der Prozessleittechnik und/oder zur Nutzung von Prozessdaten der Klärwerke und des Kanalnetzes erforderlich ist.
Ihre Daten werden auf Grundlage von Art. 6 Abs. 1 Buchstabe e) DSGVO verarbeitet.

- **Empfänger oder Kategorien von Empfängern der personenbezogenen Daten**

Ihre personenbezogenen Daten werden nicht an Dritte weitergegeben.

- **Dauer der Speicherung der personenbezogenen Daten**

Ihre Daten werden nach der Erhebung bei der Münchner Stadtentwässerung spätestens 2 Jahre nach Auftragsende gelöscht.

- **Betroffenenrechte**

Nach der DSGVO stehen Ihnen folgende Rechte zu:

- Werden Ihre personenbezogenen Daten verarbeitet, so haben Sie das Recht Auskunft über die zu Ihrer Person gespeicherten Daten zu erhalten (Art. 15 DSGVO).
- Sollten unrichtige personenbezogene Daten verarbeitet werden, steht Ihnen ein Recht auf Berichtigung zu (Art. 16 DSGVO).
- Liegen die gesetzlichen Voraussetzungen vor, so können Sie die Löschung oder Einschränkung der Verarbeitung verlangen sowie Widerspruch gegen die Verarbeitung einlegen (Art. 17, 18 und 21 DSGVO).
- Wenn Sie in die Datenverarbeitung eingewilligt haben oder ein Vertrag zur Datenverarbeitung besteht und die Datenverarbeitung mithilfe automatisierter Verfahren durchgeführt wird, steht Ihnen gegebenenfalls ein Recht auf Datenübertragbarkeit zu (Art. 20 DSGVO).
- Sollten Sie von Ihren oben genannten Rechten Gebrauch machen, prüft die öffentliche Stelle, ob die gesetzlichen Voraussetzungen hierfür erfüllt sind.
- Weiterhin besteht ein Beschwerderecht beim Bayerischen Landesbeauftragten für den Datenschutz.

- **Bereitstellungspflicht**

Die Bereitstellung der Daten ist für die Abwicklung von Aufträgen in der Prozessleittechnik und/oder zur Nutzung von Prozessdaten der Klärwerke und des Kanalnetzes erforderlich.

Wenn Sie die personenbezogenen Daten nicht bereitstellen, können Sie den Auftrag nicht erfüllen, bzw. können keine Prozessdaten der Münchner Stadtentwässerung einsehen.