5/2016
97 – 120

ZUM STAUNEN
Personalakt: Denkmal-/Datenschutz
Rainer Knyrim

DATENSCHUTZ KONKRET

Recht | Projekte | Lösungen

Chefredaktion: Rainer Knyrim

Industrie 4.0 und Datenschutz

Praxisbeitrag Industrie „Web Eye“ und See-Through-Displays

Markus Oman/ Robert Reitmann/Karin Müller

Industrie 4.0 – Auswirkungen auf Datenschutz und Arbeitsrecht

Rainer Knyrim/Boris Treml

Die Angriffsseite wird auch immer smarter

Interview mit Walter Hölblinger, Steyr Mannlicher GmbH

Microsoft Cloud Deutschland

Günther Igl

Datenschutzrechtliche Kontrollsysteme im Unternehmen

Ursula Illibauer

DSGVO: Geltendmachung der Betroffenenrechte und Auskunftsrecht

Viktoria Haidinger

Checkliste Zertifizierung Datenschutz-Gütesiegel EuroPriSe

Hans-Jürgen Pollirer

dako.manz.at

ISSN 2313-5409

MANZ

P.b.b. Verlag Manz 1230 Wien, Gutheil Schoder Gasse 17

Rainer Knyrim/Boris Treml
Rechtsanwalt und Partner bei Preslmayr Rechtsanwälte/TÜV TRUST IT TÜV AUSTRIA GMBH

Industrie 4.0 – Auswirkungen auf Datenschutz und Arbeitsrecht

Internet of Things, cyber-physisches System, Datenschutz-Folgenabschätzung, Informationssicherheitsmanagementsystem. Industrie 4.0 basiert auf Daten, die zwischen Menschen und Maschinen ausgetauscht werden. Ein fiktives Praxisbeispiel zeigt, wie Bestellungen, Serviceaufträge und Produktion von Maschinen in Zukunft automatisiert ablaufen. Bei der Vernetzung dieser Prozesse müssen die Aspekte im Bereich Datenschutz, Arbeitsrecht und Informationssicherheit ebenfalls betrachtet werden.

Einleitung

Industrie 4.0 oder auch Smart Manufacturing ist der nächste Schritt der industriellen Entwicklung, der mit der industriellen Revolution begann. Die erste industrielle Revolution basierte auf der Integration von Dampf in den Produktionsprozess, um die Maschinen anzutreiben, die zweite industrielle Revolution auf dem Konzept der Arbeitsteilung unter Verwendung des Fließbands und die dritte industrielle Revolution auf dem Einsatz von Elektronik und IT. Damit ging die Automatisierung der Produktionsprozesse zB durch Roboter einher. Die **vierte industrielle Revolution** basiert auf Daten, die über das Internet zwischen Menschen und Maschinen ausgetauscht werden.

Damit der Datenaustausch auch funktioniert, ist es notwendig, für Daten des Produktionsprozesses ein gemeinsames Netz zu schaffen und dafür Sorge zu tragen, dass die Teilnehmer im Produktionsprozess dieselbe „Sprache" sprechen. Beides findet sich im Internet wieder, nämlich ein gemeinsames Netz unter Verwendung einer standardisierten Sprache. Man spricht in diesem Zusammenhang auch vom **„Internet of Things"** und meint damit, dass eine Kommunikation unter den Gerätschaften über die Unternehmensgrenze hinweg möglich wird. Weil aber nicht nur Maschinen, sondern auch Werkzeuge und das Produkt selbst vernetzt werden, spricht man auch vom **cyber-physischen System (CPS)**.

Stand bei der zweiten Stufe der Industrialisierung die Produktionsanlage im Mittelpunkt, so steht bei der vierten Stufe der Industrialisierung das **Produkt im Mittelpunkt**; *Henry Ford* meinte: *„Jeder Kunde kann sein Auto in einer beliebigen Farbe lackiert bekommen, solange die Farbe, die er will, schwarz ist."*[1] Diese Aussage verdeutlicht wohl am besten, dass damals der gesamte Fokus auf den Produktionsprozess und nicht auf das Produkt gerichtet war. Heute hingegen bietet Volkswagen zB die Möglichkeit, das eigene Fahrzeug komplett zu personalisieren. So kann der Käufer beim Modell up! aus *„13 Außenfarben, drei Dachfarben und zehn verschiedenen Dashpad-Designs"* wählen.[2] Anders als beim Modell T von *Henry Ford* bestimmt nicht die Maschine die Produkteigenschaften, sondern teilt nun das jeweilige zu produzierende Teil der Produktionsanlage mit, in welcher Ausprägung das Produkt zu erstellen ist. Die Fähigkeit des umfassenden produktionstechnischen Datenaustauschs und der Einsatz von autonomen Entscheidungsprozessen führen zu einer digitalen

[1] Die Farbe Schwarz wurde angeblich deshalb gewählt, weil diese am schnellsten trocknet und so den Produktionsprozess beschleunigt. [2] www.motornews.at/der-neue-vw-up/ (14. 8. 2016).

Veredelung der Produktion und zu einer noch in den Kinderschuhen steckenden Steigerung der Wertschöpfung.[3]

Ein fiktives Praxisbeispiel

Das folgende Beispiel greift auf Beobachtungen der Autoren zurück. Diese haben jede Komponente in der Praxis vorgefunden, lediglich das gezeichnete Bild basiert auf den Vorstellungen der Autoren, wie sie die Zukunft vermuten lässt:

- Firma X ist ein Maschinenbauer in Österreich. Um international bestehen zu können, hat der Eigentümer beschlossen, den Bau der Maschinen anhand von in der Produktionssteuerung definierten Prozessen zu gestalten. Das Alleinstellungsmerkmal der Firma X ist, besonders schnell und zeitnah die jeweilige Maschine, individuell an Kundenbedürfnisse angepasst, fertigen zu können.
- Mitarbeiter sind mittels RFID-Technologie ortbar; im Produktionssystem ist nachvollziehbar, welcher Mitarbeiter welchen Produktionsschritt an welchem Maschinenteil getätigt hat und in welcher Produktionsphase die aktuell gefertigte Maschine ist. Die Einteilung der Mitarbeiter ist ebenfalls systemtechnisch abgebildet.
- Am frühen Nachmittag trifft eine neue Bestellung ein. Der Inhalt der Bestellung wurde von einer Maschine der Firma X getätigt. Diese Maschine ist bereits an den Kunden ausgeliefert und in Verwendung.
- Dass Aufträge automatisiert von Maschinen getätigt werden, wundert die Mitarbeiter der Firma X nicht, weil die Firma X für ihre Fehlerfrüherkennungssoftware bekannt ist. Diese Software ermöglicht, dass die beim Kunden installierte Maschine selbst erkennt, wann ein Defekt zu erwarten ist.
- Vor der Einführung der Fehlerfrüherkennung war es notwendig, dass Mitarbeiter der Firma X die Maschine in fixen vordefinierten Intervallen serviciert haben, unabhängig davon, ob das Service auch wirklich notwendig war. Heute hingegen kann die Firma X auf Grundlage dieser Fehlerfrüherkennung für die Branche noch nie dagewesene Verfügbarkeitszeiten der Produktionsanlagen garantieren, die auch vertraglich zugesichert werden. Die Erhöhung der Verfügbarkeit führt beim Kunden der Firma X zu einer Erhöhung der Produktivität und die Früherkennung von vermeintlichen Fehlern zu einem Schutz der Investition.
- Analysen haben gezeigt, dass die besten Ergebnisse erzielt werden, wenn der Mitarbeiter, der die Produktionsanlage hergestellt hat, auch mit der Herstellung der Ersatzteile beauftragt wird, weshalb der betreffende Mitarbeiter mit der Abarbeitung des Auftrags beginnt. Auf einem Tablet-Computer wird die Maschine dargestellt, für die das Ersatzteil zu fertigen ist.
- In einem ersten Schritt verbindet sich der Mitarbeiter mit der Maschine beim Kunden, für die das Ersatzteil zu fertigen ist, um nachzuvollziehen, ob der Austausch wirklich notwendig ist. Der Mitarbeiter kommt zum Ergebnis, dass der Austausch geboten ist, weshalb der Auftrag im System der Firma X erfasst wird.
- Der Mitarbeiter fasst zu Beginn das benötigte Werkzeug in der Werkzeugkammer aus, doch muss dieser weder ermitteln, welche Werkzeuge er für die Erstellung des Ersatzteils benötigt, noch, wo diese zu finden sind. Bei der Firma X ist nämlich der Werkzeugausgabeprozess so organisiert, dass die Werkzeuge ebenfalls von einem System verwaltet werden. Ein Zugriff auf Werkzeuge ohne Auftrag ist nicht möglich. Die „digitale Werkzeuglade" gibt nur Werkzeuge für im System angelegte Produktionsaufträge aus und rechnet hoch, wie lange die Werkzeuge für den Produktionsschritt benötigt werden. Diese Hochrechnung fließt in die Gesamtplanung ein.
- Überzieht ein Mitarbeiter die erwartete Dauer, so hat dieser der „digitalen Werkzeuglade" bekanntzugeben, wie lange er die Werkzeuge noch benötigt. Um eine Fehlbedienung der Werkzeuge zu vermeiden, können bestimmte Maximalwerte wie zB eine Limitierung des Drehmoments vor der Ausgabe des Werkzeugs durch die „digitale Werkzeuglade" eingestellt werden. Die Einstellung hat das System aufgrund des Arbeitsauftrags bereits vorgenommen. Der Mitarbeiter kontrolliert die Einstellungen mit den Angaben, die er auf der Datenbrille nochmals eingeblendet bekommt. Ein Spezialwerkzeug ist lediglich einmal in der Firma X vorhanden. Aufgrund der zentralen Erfassung des Werkzeugeinsatzes ist sofort bekannt, wer das Spezialwerkzeug derzeit benützt und dass es unmittelbar nach Abschluss der Tätigkeit zu übergeben ist.
- Der Rohling des zu bauenden Ersatzteils wird mit einem Gabelstapler aus dem Lager herbeigeschafft. Aufgrund einer Unachtsamkeit des Gabelstaplerfahrers kommt es hierbei zu einem Unfall. Das Fahrzeug meldet den Unfall an dessen Hersteller und der Vorfall wird automatisch im Schichtbuch protokolliert. Der Mitarbeiter übernimmt den Rohling und beginnt mit den notwendigen Arbeiten. Damit das Ersatzteil ohne weitere Anpassungen vor Ort beim Auftraggeber eingebaut werden kann, übermittelt die Maschine beim Kunden die relevanten Einstellungen und diese werden dem Mitarbeiter der Firma X zur Kenntnis gebracht.

Mit diesem Beispiel soll eine Idee von Industrie 4.0 geboten und verdeutlicht werden, wie ein CPS verstanden werden könnte. Damit Industrie 4.0 nicht zur Falle wird, ist nicht nur der Produktionsprozess so nahtlos zu gestalten, sondern es ist auch für die rechtlichen und informationssicherheitstechnischen Inhalte derselbe Reifegrad zu gewährleisten.

Für den, der diese Auseinandersetzung unterlässt, kann Industrie 4.0 aus folgenden Überlegungen sehr schnell zur Falle werden:

Personenbezogene Daten können zur Gestaltung des Produktionsprozesses oder zu einer umfassenden Überwachung verwendet werden.

Beachtung von arbeitsrechtlichen Aspekten

Damit der Mensch in den Produktionsprozess nahtlos integrierbar ist, muss dieser einer zentralen Planung jederzeit zuführbar sein. Greifbar in diesem Zusammenhang heißt, dass jeder Schritt eines Mitarbeiters durch personenbezogene Daten dargestellt wird. Abhängig davon, wie die personenbezogenen Daten verwendet werden, kann damit einerseits der Produktionsprozess gestaltet oder andererseits eine allumfassende Überwachung realisiert werden.

Gemäß § 96 ArbVG sind Maßnahmen oder technische Systeme zur Kontrolle der Arbeitnehmer nur dann in einem Betrieb,

[3] Das kann auch der Grund sein, warum der deutsche Sportartikelhersteller Adidas Teile der Produktion nach Deutschland zurückholt, *Die Welt*, Die Ära der Globalisierung steht vor dem Ende, www.welt.de/wirtschaft/article157825087/Die-Aera-der-Globalisierung-steht-vor-dem-Ende.html (28. 8. 2016).

in dem ein Betriebsrat konstituiert wurde, zulässig, wenn vor der Einführung der Maßnahme eine **Betriebsvereinbarung** abgeschlossen wurde. Obwohl die personenbezogenen Daten nicht deshalb ermittelt werden, um eine Kontrolle durchzuführen, ist eine Betriebsvereinbarung abzuschließen, weil allein die Möglichkeit der Kontrolle ausreicht. Aus diesem Grund ist der Betriebsrat vor der Einführung entsprechender Systeme einzubeziehen, weil ohne dessen Zustimmung eine Einführung der Systeme durch den Betriebsrat verhindert werden kann.

Arbeitgeber, die meinen, dass ein Betriebsrat ein Nachteil aufgrund des Mitspracherechts bei der Einführung von Industrie 4.0 ist, sollten bedenken, dass in Unternehmen, in denen kein Betriebsrat konstituiert wurde, eine **Zustimmung** iSd § 10 AVRAG von **jedem Mitarbeiter** einzuholen ist. Inhalt dieser Vereinbarung könnte sein, dass aufgrund der Datenlage keine systematische, allgemeine Mitarbeiterbeurteilung durchgeführt wird.

Ebenfalls regelungswürdig scheint, wie in einem konkreten Anlassfall der Auswertungsprozess zu erfolgen hat, also zB wann und in welcher Form der Betriebsrat zu involvieren ist. In vielen Betriebsvereinbarungen ist nämlich zu lesen, dass der Betriebsrat vor jeder **Auswertung** von **personenbezogenen Daten** zu verständigen und beizuziehen ist. Vor diesem Hintergrund ist auf § 91 Abs 2 ArbVG hinzuweisen, in dem ausdrücklich festgehalten wird, dass eine Einsicht in die Daten einzelner Arbeitnehmer lediglich dann zulässig ist, wenn der betroffene Mitarbeiter der Einsichtnahme durch den Betriebsrat zugestimmt hat, es sei denn, eine Einsichtnahme ergibt sich aus anderen Rechtsvorschriften.[4]

Beachtung von datenschutzrechtlichen und Informationssicherheitsaspekten

Am 4. 5. 2016 hat der europäische Gesetzgeber die Datenschutzgrundverordnung (DSGVO) erlassen. Diese trat am 24. 5. 2016 in Kraft und gilt ab 25. 5. 2018. Zu beachten ist, dass derzeit das DSG 2000 in Geltung ist, weshalb die entsprechende Datenanwendung iSd § 17 DSG 2000 an die Datenschutzbehörde zu melden ist. Werden personenbezogene Daten an Dritte überlassen oder übermittelt, so kann eine Genehmigungspflicht der Überlassung oder der Übermittlung vorliegen. Am 19. 7. 2016 hat der europäische Gesetzgeber die RL über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union erlassen (NIS-RL). Normiert der Gesetzgeber mit der DSGVO den Umgang mit personenbezogenen Daten, erteilt er mit der NIS-RL dem nationalen Gesetzgeber den Auftrag, sicherzustellen, dass Informationssysteme einem entsprechenden Sicherheitsniveau entsprechen und Meldung zu erstatten ist, wenn Informationen kompromittiert wurden. Art 14 und 16 NIS-RL normieren, dass Betreiber wesentlicher Dienste oder Anbieter digitaler Dienste technische und organisatorische Maßnahmen (TOM) treffen müssen, um die Sicherheit von Informationssystemen zu gewährleisten.

Unabhängig davon, ob die NIS-RL für Betriebe, die im Sinne von Industrie 4.0 organisiert und vernetzt arbeiten, anzuwenden ist, scheint es über alle Maße geboten, ein ausreichendes Maß an sicherer IT zu erlangen. Die Vernetzung von Fertigungsprozessen über Fabriken hinweg veredelt den Herstellungsprozess, doch geht mit der Vernetzung und mit dem sehr hohen Organisationsgrad auch eine immense Abhängigkeit an das Funktionieren der IT einher. Die Bedrohung lauert nicht nur außerhalb des Unternehmens durch Cyber-Attacken[5], sondern auch innerhalb des Unternehmens, etwa durch Fehlbedienung eigener Mitarbeiter des Unternehmens.

Bedrohungen der Informationssicherheit können durch Cyber-Attacken oder auch Fehlbedienung eigener Mitarbeiter entstehen.

Der Grad der zuvor verlangten Informationssicherheit kann durch die Einführung eines **Informationssicherheitsmanagementsystems** (ISMS) erreicht werden. Die Norm ISO/IEC 27001:2013 unterstützt bei dem Aufbau eines ISMS und ermöglicht eine spätere Zertifizierung der Organisation. In der Phase der Implementierung des ISMS sind die Risiken aufzudecken und einer Bewertung hinsichtlich Eintrittswahrscheinlichkeit und Auswirkungen eines Vorfalls zuzuführen. Abhängig von der Risikofreudigkeit der betreffenden Organisation sind geeignete Maßnahmen zur Risikoreduzierung zu treffen. Das ISMS hat sämtliche Prozesse und Informationen (Daten) der Organisation im Blickfeld. Haben diese Daten auch einen Personenbezug, findet derzeit das DSG 2000 und ab 25. 5. 2018 die DSGVO auf diese (personenbezogenen) Daten Anwendung. Zu diesen regulatorischen Vorgaben tritt die nationale Umsetzung der NIS-RL hinzu, wenn davon auszugehen ist, dass der Betreiber einen wesentlichen Dienst erbringt oder Anbieter von digitalen Diensten ist. Hat man bei der Einführung eines ISMS den Fokus (richtigerweise) auch auf Datenschutz gerichtet, können sehr viele datenschutzrechtliche Anforderungen abgedeckt werden. Darüber hinaus können Kenntnisse, die man im Rahmen der Einführung des ISMS gewonnen hat, im Bereich des Datenschutzes genutzt werden.[6] Bspw ist hier auf die ab 25. 5. 2018 durchzuführende **Datenschutz-Folgenabschätzung** zu verweisen. Offenkundig können die technischen Sicherheitsmaßnahmen, die im Rahmen eines ISMS etabliert wurden, auch entsprechend für die Datensicherheitsmaßnahmen, die das DSG 2000 vorschreibt, genutzt werden, um die Datensicherheit der personenbezogenen Daten zu gewährleisten.[7]

Wie im Beispiel ausgeführt, werden die Systeme über die Herstellergrenzen hinweg miteinander verbunden, um Abläufe zu automatisieren. Hat ein Teilnehmer eine **Schwachstelle** im System, kann dies zur Folge haben, dass der Produktionsprozess ins Stocken gerät oder die eigene Infrastruktur Angriffen ausgesetzt ist. Es stellt sich somit die Frage, wie sichergestellt werden kann, dass alle Teilnehmer den notwendigen Grad an Sicherheit gewährleisten können. Vorab ist zu klären, was „notwendig" heißt und welche Eigenschaften überhaupt gefordert werden. In diesem Prozess kann erneut auf die Erkenntnisse, die im Rahmen der Einführung des ISMS etwa hinsichtlich der Schutzbedarfsfeststellung, der Schutzziele oder der Datenschutz-Folgenabschätzung gewonnen wurden, zurückgegriffen werden. Ausgangspunkt dieser Erhebung sind der **Geschäftsprozess** und die hierfür verwendeten **Datenanwendungen**. Hat man den konkreten Schutzbedarf ermittelt, kann die Vertrauenswürdigkeit von Software und Hardware anhand der Normen

[4] Der Betriebsrat ist gemäß § 89 Z 1 ArbVG ua berechtigt, in die vom Betrieb geführten Aufzeichnungen über die Bezüge der Arbeitnehmer und die zur Berechnung dieser Bezüge erforderlichen Unterlagen Einsicht zu nehmen, sie zu überprüfen und die Auszahlung zu kontrollieren. Dies gilt auch für andere die Arbeitnehmer betreffenden Aufzeichnungen, deren Führung durch Rechtsvorschriften vorgesehen ist. [5] Siehe dazu Dako 2016/17 und 2016/18. [6] Siehe ErwGr 76 f DSGVO. [7] Siehe derzeit § 14 DSG 2000 und ab 25. 5. 2018 Art 32 DSGVO.

ISO/IEC 15408:2009 – „Common Criteria“[8] – (CC) oder IEC 62443 – „Industrielle Kommunikationsnetze – IT-Sicherheit für Netze und Systeme“ bewertet und geprüft werden. Hersteller wie Oracle, Microsoft oder Cisco lassen deren Systeme nach CC zertifizieren.[9] Hersteller von Industrieanlagen wie Siemens, ABB oder Honeywell wenden den Standard IEC 62443 an, um die Systemanfälligkeit für Cyber-Security-Risiken zu minimieren.

Anhand der ermittelten Anforderung an die **Vertrauenswürdigkeit** kann einerseits das eigene System auf Grundlage der Analyseergebnisse, die im Rahmen der Einführung eines ISMS gewonnen wurden, aufgebaut werden, andererseits kann auch sichergestellt werden, dass über die Produktionsgrenzen hinweg alle Teilnehmer an einem CPS ihr Informationssystem so aufgebaut haben, dass eine einheitliche Vertrauenswürdigkeit der Informationssysteme in einem CPS gegeben ist, obwohl unterschiedliche Systeme zum Einsatz kommen.

Die Verpflichtung zur Einhaltung der zugesicherten Vertrauenswürdigkeit ist vertraglich zu regeln. Der Nachweis, dass die Vertrauenswürdigkeit auch eingehalten wird, kann durch **Audits oder Zertifizierungen** erbracht werden. Ebenso sind zu installierende Prozesse einer vertraglichen Regelung zuzuführen. Sieht § 24 Abs 2a DSG 2000 eine Data Breach Notification Duty vor, also die Pflicht, den Betroffenen von einer unrechtmäßigen Verwendung seiner personenbezogenen Daten zu informieren, ist eine Pflicht zur Information im Umfeld von Industrie 4.0 „nur“ auf die allgemeinen Grundsätze der Schutz- und Sorgfaltspflichten zurückzuführen. Um Sicherheit zu erlangen, sollte der Informationssicherheitsprozess einer vertraglichen Regelung zugeführt werden; dieser Prozess ist im Rahmen des ISMS zu implementieren.

Fazit

Industrie 4.0 basiert auf der Verzahnung und Vernetzung der Produktionsprozesse über Herstellergrenzen hinweg; im Optimalfall wird tatsächlich ein CPS implementiert. Neben dieser operativen Produktionsverschmelzung müssen die Themenbereiche Datenschutz, Arbeitsrecht und Informationssicherheit ebenfalls ganzheitlich betrachtet werden.

Dako 2016/70

[8] www.commoncriteriaportal.org/products/ (4. 9. 2016).
[9] Links siehe Fact Box am Ende des Beitrags.

Zum Thema

Über die Autoren

RA Dr. Rainer Knyrim ist Rechtsanwalt und Partner bei Preslmayr Rechtsanwälte. Kontakt: Tel: +43 (0)1 5331695, E-Mail: knyrim@preslmayr.at; Internet: www. preslmayr.at
Boris Treml, LL.M., ist Senior Consultant bei TÜV TRUST IT TÜV AUSTRIA GMBH. E-Mail: boris.treml@it-tuv.com; Internet: www.it-tuv.com

Links Software und Hardware

- Oracle: www.oracle.com/technetwork/topics/security/oracle-common-criteria-095703.html (4. 9. 2016)
- Microsoft: https://msdn.microsoft.com/en-us/library/dd229319.aspx (4. 9. 2016)
- Cisco: www.cisco.com/c/en/us/solutions/industries/government/global-government-certifications/common-criteria.html (4. 9. 2016)
- Siemens: www.siemens.com/digitalisierung/cyber-security.html (20. 9. 2016)
- ABB: ABB technik, 3/12/64, https://library.e.abb.com/public/e0de281f67298983c1257a79003f3fc4/ABB%20Technik%203-2012_72dpi.pdf (12. 11. 2016)
- Honeywell: www.honeywell.com/newsroom/pressreleases/2015/04/honeywell-technology-first-to-proactively-manage-cyber-security-risk-for-industrial-sites (12. 11. 2016)

Fact Box

ISO-Standardisierung für Industrie 4.0

Es gibt derzeit noch keine ISO-Standardisierung für Industrie 4.0, die aber geboten scheint, weil die Vorteile nur dann gehoben werden können, wenn die Akteure (Maschinen, Produkte) dieselbe Sprache sprechen. Deshalb hat die International Standard Organization (ISO) eine Strategiegruppe eingerichtet; www.din.de/de/forschung-und-innovation/industrie4-0/industrie-4-0-iso-richtet-strategiegruppe-ein-66482 (13. 8. 2016).

MANZ