

# Office 365 und MS International Cloud

## Einführung um jeden Preis?

### Erhebliche Datenschutz-Bedenken des Gesamtbetriebsrats

Der Wechsel auf die neueste Version des Office-Pakets von Microsoft steht vor der Tür. In etlichen Unternehmen ist die Umstellung auf »Office 365« in Vorbereitung oder bereits vollzogen. Auch Fraunhofer bereitet diese Umstellung vor. Der Gesamtbetriebsrat (GBR) hat jedoch grundsätzliche Zweifel, ob der vorgesehene Betrieb von Office 365 in der International Cloud von Microsoft (MS International Cloud) von den [europäischen Datenschutznormen \(DSGVO\)](#) gedeckt ist und lehnt dieses Betriebsmodell daher ab. Infolge dessen verweigert der GBR derzeit die erforderliche Zustimmung zur Einführung von Office 365 in der MS International Cloud bei Fraunhofer.

Da über die Chancen und Risiken von Office 365 nicht nur in IT-Kreisen, sondern auch in der Belegschaft kontrovers diskutiert wird – auch, weil einige Kunden und Projektpartner das Softwarepaket einsetzen, andere hingegen sich skeptisch bis ablehnend verhalten – möchte der GBR seine kritische Position Fraunhofer-öffentlich darstellen und begründen.

### Cloud-Systeme - heiter bis wolkig

Seit einigen Jahren findet auf breiter Front die Einführung von Cloud-Systemen statt. Auch bei Fraunhofer wird bereits seit mehreren Jahren die »Fraunhofer Cloud« angeboten, in der die Institute Server und Services anmieten können. Beispiele für in der Fraunhofer Cloud betriebene Services



sind das Gefahrstoffverwaltungssystem »GEVIS III«, das Repository für Forschungsdaten »Fordatis«, aber auch verschiedene Webserver der Institute. Ein Fraunhofer-weit verfügbarer Cloud-Speicher wird bereits seit längerem angeboten. Die aktuelle Version basiert auf der OpenSource-Software »[owncloud](#)«.

Die Server und Services der Fraunhofer Cloud werden bisher von der Fraunhofer-Gesellschaft in Eigenregie im internen Netz betrieben. Das bedeutet, dass die Hoheit über die verwendete Hard- und Software und – vielleicht noch wichtiger – die Hoheit über die verarbeiteten und gespeicherten Daten in den eigenen Händen liegt. Dennoch können die Fraunhofer Cloud-Systeme bei entsprechender Konfiguration auch von außen, also aus dem Internet, erreicht werden.

Seit einiger Zeit werden Cloud-Systeme von spezialisierten Unternehmen an-

geboten, die sowohl Rechnerkapazität als auch Speicherplatz gegen Entgelt zur Verfügung stellen. Prominentester Anbieter von Cloud-Diensten ist sicherlich »Dropbox«. Dies ist ein reiner Cloud-Speicher, der gerne zum Datenaustausch genutzt wird. Für Fraunhofer-Daten ist Dropbox allerdings aus Gründen des Daten- und Geheimschutzes nicht geeignet und darf deshalb dienstlich nicht genutzt werden.

Ein weiterer bekannter Cloud-Anbieter ist »Amazon«. Amazon ist nicht nur als Online-Kaufhaus bekannt, sondern bietet Cloud-Speicher und Rechner-Ressourcen in fast beliebig konfigurierbarer und virtualisierter Ausstattung an. Größere Anbieter solcher Cloud-Dienste in Deutschland sind Firmen wie beispielsweise die Deutsche Telekom, Strato, 1&1, Hetzner oder Nextcloud. Nextcloud setzt unter anderem die »[Bundescloud](#)« für Ministerien und andere Behörden um.

## Auch die Software wird wolkig

Microsoft als Anbieter des Office-Pakets, Adobe mit seiner Creative Suite, aber auch SAP mit seinem ERP-System haben, ebenso wie weitere große Softwareanbieter, in den letzten Jahren mit der Einführung des Mietmodells und dem Betrieb der Anwendungen in der Cloud einen grundlegenden Wandel eingeleitet.

Für die Anbieter ergeben sich daraus Vorteile bei der Kontrolle der Nutzerlizenzen, da Raubkopien faktisch ausgeschlossen sind. Sie können allen Kunden zeitgleich Updates und neue Releases bereitstellen und so den Support für ältere Software-Versionen vermeiden. Leider enthält die Cloud-Software zunehmend attraktive Funktionen, die nur beim Betrieb in der vom Anbieter bereitgestellten Cloud nutzbar sind. Werden überhaupt lokal installierbare Versionen angeboten, fehlen diese Funktionen häufig.

Der Weg in die Cloud hat für die Nutzer einige Nachteile, denn deren Daten können zumindest während der Bearbeitung in der Cloud nicht mehr auf eigenen Systemen gehalten werden. Auch müssen alle Updates und Release-Wechsel mit in der Regel veränderten Funktionen ungefragt mitgemacht werden – allenfalls mit etwas Zeitverzug. Die faktische Hoheit über die eingesetzten Software-Versionen, deren Funktionsumfang und auch über die Daten geht verloren. Sie kann in Verträgen zwar normativ, aber in der Regel nur ohne echte Einfluss- und Kontrollmöglichkeiten für die Nutzer nachgebildet werden. Auch besteht das Risiko der Einstellung ganzer Dienste oder einzelner Funktionen wie unlängst auf Veranlassung der US-Regierung durch Adobe in [Venezuela](#).

## Ursprüngliches Betriebskonzept für Office 365

Fraunhofer plant schon seit längerem, Office 365 cloudbasiert einzusetzen. Ursprünglich war der Betrieb in der Microsoft Azure Deutschland Cloud (MS National Cloud) vorgesehen. Die MS National Cloud wurde durch den Datentreuhänder T-Systems in Deutschland und damit ohne direkte

Zugriffsmöglichkeit für Microsoft betrieben. Für dieses Betriebskonzept, das der GBR wegen des hohen Datensicherheits- und Datenschutzniveaus befürwortete, waren mit dem Arbeitgeber bereits Regelungen in der Gesamtbetriebsvereinbarung »Grundsätze des IT-Einsatzes – generische IT-Lösungen« (GBV »IT-Grundsätze«) vereinbart worden.

Als Fraunhofer nach Beendigung eines längeren Lizenzrechtsstreits mit Microsoft Mitte 2018 den Vertrag über die Nutzung der MS National Cloud abschließen wollte, hatte Microsoft

gelhaften Datensouveränität wurde der vollständige Einsatz von Office 365 in der MS International Cloud jedoch ausdrücklich nicht empfohlen.

## Überraschungspaket des Vorstands

Der zuständige Fachausschuss des GBR, der GBR-A72 »Grundsätze des IT-Einsatzes« hatte bereits Ende 2018 mit der Arbeitgeberseite mehrere Verhandlungstermine im ersten Quartal 2019 vereinbart, um zügig zu Regelungen für die noch im Dezember 2018 als wahrscheinlich geltende hy-



kurz zuvor den Vertrieb beendet, so dass dieses Betriebsmodell für Neukunden nicht mehr verfügbar war.

Nach einigen konzeptionellen Überlegungen der zuständigen Abteilung C7 »Kommunikationsmanagement« der Zentrale und beratenden Gesprächen mit dem GBR wurde Ende 2018 auf der Basis einer Analyse des Fraunhofer-Informationssicherheitskoordinators (ISK) dem Vorstand ein »hybrides« Betriebskonzept empfohlen. Dies beinhaltete, Office 365 teilweise in der MS International Cloud mit Speicherorten in der EU und teilweise in den Räumen und auf Systemen von Fraunhofer (on premises) zu betreiben.

Es wurden mehrere Szenarien entwickelt, die sich darin unterschieden, welche Dienste in welchem Umfang on-premises betrieben werden sollten und welche in der Cloud. Wegen der man-

bride Lösung zu kommen. Während der ersten Verhandlung Ende Januar 2019 wurde dem GBR-A72 überraschend mitgeteilt, dass der Vorstand sich entgegen der Empfehlung des ISK und der Hauptabteilung 3C »IuK-Management« der Zentrale für die unbeschränkte Nutzung von Office 365 in der MS International Cloud entschieden habe, und somit ein hybrider Betrieb einzelner Office 365-Komponenten keine Rolle mehr spielen sollte. Der GBR-A72 machte daraufhin umgehend grundlegende datenschutzrechtliche Bedenken geltend.

## US-CLOUD Act und andere Ärgernisse

Die MS International Cloud wird mit einer zentralen Authentifikation und verschiedenen Office 365-Diensten – darunter die für Nutzer besonders



attraktive Anwendung »Teams« für Terminabsprachen, Telefonate, Video-Konferenzen und kollaboratives Arbeiten am selben Dokument – ausschließlich in der Cloud in Microsofts eigenen US-Rechenzentren angeboten. Der Zugriff durch außerhalb von Europa beheimatete Niederlassungen und Subunternehmen ist dabei nicht ausgeschlossen. Auf Kundenwunsch können bei manchen Diensten die sogenannten ruhenden Daten mittlerweile in welt-

weit verteilten, auch europäischen Rechenzentren gespeichert werden, soweit heute bekannt nicht jedoch während des Bearbeitungsvorgangs. Dann befinden sich die Daten außerhalb des Geltungsbereichs der DSGVO.

Da sich hierunter auch personenbezogene Daten von Arbeitnehmer\*innen, Projektpartnern und Kunden befinden, hält der GBR dies nicht für DSGVO-konform.

Weitere Datenschutzverletzungen sieht der GBR wegen des [US-Clarifying Lawful Overseas Use of Data Acts](#) (CLOUD Act). Kurz gesagt erlaubt dieses Gesetz US-Behörden auf Kundendaten eines US-Unternehmens, das elektronische Kommunikations- oder Remote-Computing-Dienste anbietet, zuzugreifen, selbst wenn die Daten außerhalb der USA oder bei Auslandstöchtern gespeichert sind. Dabei kann sogar verboten werden, die Kunden über den erfolgten Zugriff zu informieren.

Der Betrieb von Office 365 in der MS International Cloud ließe genau dies zu, selbst wenn die ruhenden Daten auf Microsoft-Servern in Irland, den Niederlanden oder zukünftig auch in Deutschland gespeichert würden.

Als datenschutzrechtlich problematisch stuft der GBR weiter ein, dass sich Microsoft in den [MS Online Services Terms](#) ausbedungen hat, den Support auch durch Niederlassungen und Subunternehmen in Drittstaaten erbringen lassen zu können. Der Support beinhaltet den Zugriff auf Diagnosedaten, es können aber auch Kundendaten einbezogen sein. Die Vertragsformulierungen zur Weitergabe der Kundendaten decken sich zudem genau mit den Konditionen, die für die Erfüllung der Anforderungen des CLOUD Act erforderlich sind.

Bestärkt wird der GBR in seiner Kritik durch etliche Publikationen, in denen über erhebliche Bedenken der Datenschutzbehörden gegen die Praxis von Microsoft berichtet wird, Telemetrie- und Supportdaten – das sind Daten, die das Verhalten der User und der Software beschreiben – ohne wirksame Einschränkungen in die USA oder andere Drittländer zu übermitteln. Teilweise wurden deshalb Nutzungsverbote für den behördlichen Einsatz ausgesprochen, die auch nach Anpassungen an der Software bisher nicht endgültig aufgehoben wurden.

Die DSGVO-Konformität von Office 365 als Cloud-Anwendung und der Verlust der Datensouveränität werden ebenfalls kritisch diskutiert. Im Forschungsumfeld wird erwogen, sich von kommerziellen Cloud-Anbietern zu lösen oder die Nutzung auf das Nötigste zu beschränken ( --> [siehe Kasten](#) ).

## ■ Auswahl aktueller Veröffentlichungen zum Thema

- [Bundesregierung treibt den Aufbau einer Europa-Cloud voran](#), 22.07.2019
- [Justizministerium weist auf Rechtsrisiken bei US-Datenzugriff hin](#), 17.05.2019
- [Give me all your data: US CLOUD Act & Australian »Decryption« Bill vs. the GDPR](#), 19.12.2018
- [Bewerbungsdaten in US-Cloud – Verschlüsselung ist Pflicht](#), 19.03.2019
- [Office 16 und Office 365 – Datenschutz-Handlungsbedarf im Unternehmen](#), 02.01.2019
- [Windows 10 und Office 365: Microsoft verspricht Verbesserungen beim Datenschutz](#), 07.05.2019
- [Die Datenschutz-GAUs in Office 365 - Loch an Loch](#), 05/2019
- [Marktanalyse: Microsoft-Abhängigkeit führt zu »Schmerzpunkten« beim Bund](#), 19.09.2019
- [Krieg der Daten – Kollision von EU DSGVO und US CLOUD Act](#), 28.03.2018
- [Digitale Souveränität: Innenministerium für »großen Wurf« gegen Microsoft & Co.](#), 28.05.2019
- [CERN wechselt von Microsoft- zu Open-Source-Software](#), 16.06.2019; ausführlicher: [Migrating to open-source technologies](#), 12.06.2019

## Datenschutzfolgenabschätzung und Hinweise des Bundesdatenschutzbeauftragten

Die GBR-Vorsitzenden haben vor diesem Hintergrund am 20.02.2019 ihre Bedenken in einem ersten Schreiben an den zuständigen Fraunhofer-Vorstand (Vorstandsbereich C »Controlling und Digitale Geschäftsprozesse«) formuliert. Ein anschließendes Gespräch und ein weiterer Briefwechsel führten zu keiner Verständigung. Vereinbart wurde jedoch, für den Einsatz von Office 365 in der MS International Cloud gemäß Art. 35 DSGVO eine [Datenschutzfolgenabschätzung](#) (DSFA) in Auftrag zu geben.

Parallel wandte sich der GBR mit der Bitte um eine datenschutzrechtliche Einschätzung an den Bundesbeauftragten für Datenschutz und Informationsfreiheit (BfDI), an das Bundesamt für Sicherheit in der Informationstechnik (BSI) und etwas später auch an den bayerischen Landesbeauftragten für den Datenschutz (BayLDA).

Die DSFA des Vorstands liegt dem GBR seit Mitte Mai 2019 vor. Der beauftragte Anwalt vertritt darin die Ansicht, dass Risiken für den Umgang mit personenbezogenen Arbeitnehmerdaten in der von ihm vorgesehenen Konfiguration von Office 365 in der MS International Cloud zwar in gewissem Umfang bestünden, diese Risiken aber beherrschbar seien. Schließlich seien illegitime Zugriffe so geschäftsschädigend, dass Microsoft US-Behörden einen Zugriff auf in der MS International Cloud gespeicherte Daten nicht gewähren würde. Zudem sei der CLOUD Act wegen fehlender bilateraler Abkommen mit Deutschland oder der EU ohne explizite richterliche Genehmigungen nicht anwendbar. Wegen zunächst ausstehender Auskünfte von Microsoft wurde die [DSFA zum 25.09.2019](#) nochmals ergänzt und in den Grundaussagen weiter entschärft.

Die Argumentation des Vorstands und der DSFA überzeugte den GBR nicht, zumal mittlerweile der [BfDI mit Schreiben vom 17.05.2019](#) auf die GBR-Anfrage geantwortet hatte. Zwar stellt der BfDI fest, dass er für Fraunhofer als Aufsichtsbehörde nicht zuständig sei – dies ist das [BayLDA](#).

Der BfDI teilte in seinem Schreiben jedoch mit, dass Bundesbehörden wegen des Verstoßes gegen die DSGVO nicht nur die Nutzung der MS International Cloud, sondern sogar die Nutzung der MS-Software auf eigenen Systemen nicht erlaubt sei. Die MS-Software übermittele permanent Telemetrie-Daten an Microsoft, was nicht unterbunden werden könne.

## Anwaltliche Stellungnahme des GBR zur DSFA

Entsprechend seiner Grundüberzeugung, mit dem Vorstand keine Regelung vereinbaren zu wollen, die einen Rechtsverstoß beinhaltet, beauftragten die GBR-Vorsitzenden Ende Mai 2019 im Benehmen mit der Arbeitgeberseite die Kanzlei »schwegler rechtsanwälte« in Berlin mit der Klärung der aus GBR-Sicht nach wie vor offenen Rechtsfragen – insbesondere, ob ein DSGVO-konformer Betrieb von Office 365 in der MS International Cloud überhaupt möglich ist. Die [Stellungnahme der Kanzlei »schwegler rechtsanwälte«](#) ist von der ehemaligen Justizministerin Prof. Dr. Herta Däubler-Gmelin unterzeichnet und liegt dem GBR und auch dem Vorstand seit Anfang Juli 2019 vor.

Die Stellungnahme bestärkt den GBR in seiner Rechtsauffassung: Wegen des US-CLOUD Acts und zusätzlich einer sogenannten Executive Order des US-Präsidenten vom 27.01.2017 finde ein nicht gerechtfertigter Eingriff in das Grundrecht der Arbeitnehmer\*innen auf informationelle Selbstbestimmung, das Grundrecht auf Schutz der Kommunikation sowie das Grundrecht auf effektiven Rechtsschutz als Ausprägung des im Grundgesetz und im EU-Recht verankerten Rechtsstaatsprinzips statt.

Auch die Abwägung des legitimen Arbeitgeberinteresses an der Nutzung der Office 365-Anwendungen und -Dienste in der MS International Cloud gegenüber den Rechten der Arbeitnehmer\*innen führe zu keinem anderen Ergebnis. Die allgemeine Handlungsfreiheit des Arbeitgebers (Art. 2 Abs. 1 [Grundgesetz](#) (GG)) und die spezielle unternehmerische Betätigungsfreiheit (Art. 12 Abs. 1 GG) müssten hinter die ebenfalls grundgesetzlich ge-

schützten aber gewichtigeren Rechte der Betroffenen auf informationelle Selbstbestimmung, auf geschützte Kommunikation und auf Rechtsbehelf zurücktreten. Dies gelte auch deshalb, weil alternativ zum Einsatz von Office 365 in der MS International Cloud mildere Mittel zur Verfügung stünden, die den Interessen von Fraunhofer als Arbeitgeber zwar nicht vollständig, aber ausreichend Rechnung trügen und daher zumutbar seien.

Insgesamt wird die DSGVO-Konformität des Office 365-Betriebs in der MS International Cloud klar verneint.

## Konfliktlösung in der Einigungsstelle angestoßen

Die unterschiedlichen Auffassungen von Vorstand und GBR bestehen aktuell fort. Die Einführung und der Betrieb von Office 365 in der MS International Cloud setzen gemäß [Betriebsverfassungsgesetz](#) (BetrVG) eine gültige Gesamtbetriebsvereinbarung voraus, deren Verhandlung angesichts der unterschiedlichen Rechtsauffassungen gescheitert ist.

Das BetrVG sieht für einen solchen Konfliktfall eine paritätisch besetzte »Einigungsstelle« vor, in der unter Vorsitz und Moderation einer unabhängigen Person – meist eines Arbeitsrichters – nach für beide Seiten tragbaren Lösungen gesucht wird. Kann auf dem Verhandlungsweg kein akzeptabler Kompromiss gefunden werden, fällt die Einigungsstelle mit der Stimme des Vorsitzenden einen sogenannten »Spruch«, der dann die Wirkung einer Gesamtbetriebsvereinbarung hat.

Die Betriebsparteien haben sich am 21.08.2019 darauf verständigt, eine solche Einigungsstelle zur Einführung von Office 365 einzurichten. Bis Ende des Jahres 2019 sind zunächst sechs Termine anberaumt, um zu einer Gesamtbetriebsvereinbarung zu kommen. Welchen Inhalts diese Regelung sein wird, ist aus heutiger Sicht kaum abzuschätzen, denn dem GBR vorliegende Betriebsvereinbarungen anderer Unternehmen setzen sich mit der von ihm aufgeworfenen Grundsatzfrage nicht auseinander. Der GBR wird über den weiteren Fortgang berichten. ■

## Kernaussagen der Stellungnahme der Kanzlei »Schwegler Rechtsanwälte«, Berlin

- Art. 25 DSGVO »Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen« – privacy by design / privacy by default – ist nicht wie vom Vorstand angenommen »deklaratorischer« Natur, sondern zwingend anzuwendendes Recht und bereits bei der Wahl der Mittel einer Verarbeitung personenbezogener Daten umzusetzen. Diese Norm hat einen eigenen Regelungscharakter, der im bisherigen Datenschutzrecht (BDSG alt) nicht enthalten war.
- Ob bei der Nutzung von Office 365 in der MS International Cloud der Schutz vor einem automatisierten Profiling, der von Art. 22 DSGVO »Automatisierte Entscheidungen im Einzelfall einschließlich Profiling« gefordert wird, umsetzbar ist, kann ohne umfassende technische Analysen nicht beurteilt werden. Dieser Schutz muss bei einem DSGVO-konformen Betrieb jedoch gewährleistet sein.
- Der CLOUD Act und zusätzlich die Executive Order des US-Präsidenten vom 27.01.2017, die den Schutz von Nicht-US-Bürgern im CLOUD Act aufhebt, schließen eine DSGVO-konforme Verarbeitung personenbezogener Daten in der MS International Cloud aus. Das mit dem CLOUD Act einhergehende Verbot der Unterrichtung der von der Offenlegung der Daten betroffenen Personen hebt das Grundrecht auf effektiven Rechtsschutz des Art. 47 der [Charta der Grundrechte der Europäischen Union](#) (GRCh) und Art. 19 Abs. 4 GG i. V. m. Art. 2 Abs. 1 GG aus. Beides sind Ausprägungen des Rechtsstaatsprinzips und müssen uneingeschränkt gelten. Ein Eingriff in diese Grundrechte ist nicht zulässig und kann nicht gerechtfertigt werden.
- Art. 48 DSGVO »Nach dem Unionsrecht nicht zulässige Übermittlung oder Offenlegung« verlangt für jede Übermittlung oder Offenlegung personenbezogener Daten an eine Behörde eines Landes außerhalb des Geltungsbereichs der DSGVO – sog. Drittland – eine internationale Übereinkunft. Ein Gesetz oder eine andere bindende Übereinkunft, die es dem Arbeitgeber gestattet, personenbezogene Daten an US-Behörden oder die eines anderen Drittlands zu übermitteln, existiert nicht. Werden personenbezogene Daten von Fraunhofer-Beschäftigten beispielsweise auf Grundlage des CLOUD Act offengelegt, liegt ein Verstoß gegen Art. 48 DSGVO vor.
- Durch die Verschlüsselung der übermittelten Daten wird das Schutzniveau nicht ausreichend erhöht, da den Interessierten ausreichend Zeit und Ressourcen zur Entschlüsselung zur Verfügung stehen. Werden also personenbezogene Daten entgegen der Regelung in Art. 48 DSGVO an Behörden in Drittländern übermittelt, liegt auch dann eine unzulässige Übermittlung und damit ein Verstoß gegen die DSGVO vor, wenn die Daten verschlüsselt oder pseudonymisiert sind.
- Die Datenübermittlung in andere Drittländer als die USA kann zulässig sein, wenn die Vorgaben des Art. 46 DSGVO »Datenübermittlung vorbehaltlich geeigneter Garantien« nachweislich umgesetzt werden. Solche Nachweise liegen derzeit nicht vor.
- Die vollständige Umsetzung der DSGVO führt in der Regel dazu, dass die Anforderungen des [Gesetzes zum Schutz von Geschäftsgeheimnissen](#) (GeschGehG) erfüllt sind, um den Schutz von Geschäftsgeheimnissen wirksam werden zu lassen. US-Behörden können jedoch auf Grundlage des CLOUD Act auch Geschäftsgeheimnisse herausverlangen. Gleiches gilt für IP- und urheberrechtsrelevante Daten, die ebenfalls US-Behörden zur Kenntnis gelangen können.
- Gegen die Nutzung von Office 365 in der MS International Cloud für vertrauliche Informationen – u. a. durch betriebsverfassungsrechtliche Gremien – bestehen durchgreifende datenschutzrechtliche Bedenken.



 **Fraunhofer**  
Gesamtbetriebsrat

### Impressum

#### Herausgeber

Fraunhofer Gesamtbetriebsrat  
Breslauerstr. 48, 76139 Karlsruhe  
E-Mail: [gbr-vorsitz@fraunhofer.de](mailto:gbr-vorsitz@fraunhofer.de)  
<http://gesamtbetriebsrat.fraunhofer.de>

#### Verantwortliche Redakteure

Kerstin Hölscher (UMSICHT Oberhausen)  
Guido Huppertz (INT)  
Wolfgang Lux (IPA Stuttgart)  
Winfried Müller (ISC Würzburg)  
Stefan Rughöft (FOKUS Berlin)  
Dominik Toussaint (ISI Karlsruhe)

#### Satz & Layout

Dominik Toussaint (ISI Karlsruhe)

© Fraunhofer Gesamtbetriebsrat  
Karlsruhe, Oktober 2019