Einholung der Zustimmung des Betriebsrats zum Erfassen von E-Mails und elektronischen Dokumenten mithilfe EnCase® Enterprise und EnCase® eDiscovery

von Patrick Burke
Anwalt, Reed Smith LLP
pburke@reedsmith.com[1]

ReedSmith

I. Kurzfassung

Deutsche Unternehmen sind verpflichtet, Daten aus rechtmäßigem Geschäftsinteresse des Unternehmens zu erfassen, darunter zur Einhaltung von Verpflichtungen, um Zuwiderhandlungen nachzugehen, zur Zuerkennung von Ansprüchen und zum Schutz personenbezogener Daten von Kunden vor Missbrauch. Unternehmen, die EnCase® Enterprise oder EnCase® eDiscovery[2] zur Durchsuchung und Erfassung von E-Mails und elektronischen Dokumenten von Angestellten in Deutschland verwenden möchten, müssen als entscheidende Voraussetzung dafür die Zustimmung des unternehmenseigenen Betriebsrats einholen. Die deutschen Betriebsräte genießen einen ausgezeichneten Ruf als strenge Hüter des Schutzes der Privatsphäre der Mitarbeiter, lehnen teilweise Bestrebungen des Unternehmens ab, Mitarbeiterdaten zu durchsuchen, und machen Rechte und Schutzmaßnahmen von Angestellten in Deutschland gemäß der Datenschutzrichtlinie der Europäischen Union von 1995[3] und der bundes- und landesrechtlichen Datenschutzgesetze, die die Richtlinie umsetzen, geltend.

Es ist jedoch nicht ungewöhnlich, dass deutsche Betriebsräte der Datenerfassung zustimmen, wenn die Privatsphäre der Mitarbeiter angemessen geschützt wird. In der Tat erkennen die europäischen Datenschutzgesetze an, dass es ein Gleichgewicht zwischen dem Grundrecht auf Privatsphäre und den rechtmäßigen Geschäftsinteressen und gesetzlichen Verpflichtungen geben sollte. Der Verfasser dieses Dokuments war bei einer Reihe von erfolgreichen Anfragen an deutsche Betriebsräte beteiligt. Der Schlüssel zu diesem Erfolg liegt in einer fundierten und feinfühligen Präsentation vor dem Betriebsrat und dem Angebot einer Erfassungsmethodik, die den Schutz von Mitarbeiterrechten einschließt. EnCase®-Produkte können bei dieser Rechtsschutzmethodik Hilfestellung leisten.

In diesem Whitepaper werden folgende Fragen behandelt:

- Was ist ein deutscher Betriebsrat und wie funktioniert er?
- Auf welche deutschen Datenschutzregelungen können Betriebsräte ihre Einwände stützen?
- Welche Schritte kann ein Unternehmen ergreifen, um für die Möglichkeiten der Datenerfassung mit EnCase® die Zustimmung eines deutschen Betriebsrats zu erhalten?

II. Betriebsräte in Deutschland

Betriebsräte sind bereits seit Anfang des 20. Jahrhunderts fester Bestandteil der deutschen Wirtschaft und Industrie. Die erste Verfügung eines Betriebsrats wurde nach dem Ersten Weltkrieg erlassen und besteht seitdem in unterschiedlichen Ausführungen. Das geltende Recht ist im Betriebsverfassungsgesetz von 1972 verankert und gilt für Privatunternehmen mit mehr als fünf fest angestellten und wahlberechtigten Mitarbeitern.[4]

Betriebsräte werden durch demokratische Prozesse gegründet. Kandidaten für Betriebsräte müssen eine bestimmte Anzahl von Unterschriften ihrer Kollegen vorweisen können, um wählbar zu sein.[5] Auch Gewerkschaften können Kandidaten zur Wahl aufstellen, ihre Mitglieder jedoch nicht dazu zwingen, auf bestimmte Weise abzustimmen.[6] Die Betriebsratsmitglieder werden direkt durch die Angestellten des Unternehmens in geheimer Wahl gewählt, wobei die Angestellten jedoch nicht zur Wahl verpflichtet sind.[7] Gewählte Mitglieder haben ihr Amt üblicherweise 4 Jahre inne.[8] Die Größe des Betriebsrats hängt von der Anzahl der Angestellten des Unternehmens ab und muss anteilig bestimmte Beschäftigungsgruppen, z. B. Frauen, widerspiegeln.[9]

Nach dem Betriebsverfassungsgesetz hat der Betriebsrat das Recht, Angelegenheiten, die die Unternehmensstruktur betreffen, Personalentscheidungen, Richtlinien zum Arbeitsplatz und individuellem Verhalten innerhalb des Unternehmens mitzubestimmen.[10] Die Rechte eines Betriebsrats können wie folgt kategorisiert werden:

- **Information:** Das Recht auf Information zur Umsetzung oder Änderung von Praktiken oder Richtlinien im Unternehmen. Ggf. muss der Arbeitgeber hierzu Dokumentation bereitstellen.
- **Beratung und Zusammenarbeit:** Das Recht, mit der Geschäftsführung zu beraten und zusammenzuarbeiten, um das jeweilige Thema gemeinsam zu diskutieren und zu entwickeln.
- **Vetorecht:** Das Recht, bestimmte Managemententscheidungen zu blockieren.

Der Arbeitgeber ist verpflichtet, den Betriebsrat vollständig zu Angelegenheiten hinsichtlich des operativen Geschäfts und der Personalplanung zu informieren, sodass sich der Betriebsrat an der Erarbeitung der Unternehmenspolitik beteiligen kann.[11] Durch diese Zusammenarbeit mit dem Betriebsrat vermeidet die Geschäftsführung mögliche Streitigkeiten und erfährt von relevanten Bedenken oder unterbreitet Vorschläge. Für die Beschlüsse des Betriebsrats ist eine beschlussfähige Mehrheit von 50 % erforderlich, und die Beschlüsse werden durch eine einfache Mehrheit angenommen, sofern gesetzlich nichts anderes vorgeschrieben ist.[12] Der Betriebsrat und die Geschäftsführung können formelle oder formlos gültige und verbindliche Vereinbarungen miteinander treffen.[13] Formelle Vereinbarungen sind für den Arbeitgeber und die Angestellten sofort verbindlich. Bei formlosen Vereinbarungen sind zusätzliche Schritte erforderlich, z. B. die Änderung eines Arbeitsvertrags. Der Betriebsrat darf nur für diejenigen Bereiche des Geschäftsbetriebs Betriebsvereinbarungen abschließen, für die das Betriebsverfassungsgesetz Mitbestimmungsrechte einräumt. Tarifvertragsbestimmungen zwischen Arbeitgeberverbänden und Gewerkschaften haben absoluten Vorrang gegenüber Betriebsvereinbarungen, selbst wenn Letztere günstiger für die Arbeitnehmerschaft sind.[14]

Können Streitigkeiten zwischen dem Betriebsrat und der Geschäftsführung nicht einvernehmlich gelöst werden, können die Parteien Unterstützung beim Vermittlungsausschuss anfordern, einem Gremium mit Schieds- und Vermittlungsaufgaben.[15] Sofern beide Parteien im Voraus festlegen, sich an dessen Entscheidung zu binden, ist die Entscheidung des Vermittlungsausschusses endgültig und verbindlich und kann nur dann angefochten werden, wenn der Ausschuss gegen allgemeine Rechtsgrundsätze verstoßen hat.[16]

III. Deutsche Datenschutzregeln

Wenn ein Betriebsrat Rechte geltend macht, die Methodik zur Erfassung von Mitarbeiterdaten zu genehmigen oder diese abzulehnen, machen sie dabei teilweise die Ansprüche von Arbeitnehmern gemäß dem Gesetz der Europäischen Union (EU), der Bundesrepublik Deutschland und den Datenschutzgesetzen der einzelnen Bundesländer geltend. Auch wenn alle EU-Mitgliedstaaten die Vorgaben der EU-Richtlinie einhalten müssen, steht es jedem Mitglied frei, individuelle Gesetzgebungen innerhalb seines eigenen Landes umzusetzen, um diese Vorgaben zu erreichen.[17]

Die EU-Datenschutzrichtlinie lässt ein Abwägen des rechtmäßigen Geschäftsinteresses des Unternehmens gegenüber dem Schutz der Privatsphäre der Mitarbeiter zu.[18] Best Practices haben gezeigt, dass dieser Ausgleich am besten erreicht wird, wenn zur Verarbeitung der Daten die am wenigsten eingriffsintensiven praktikablen Vorgehensweisen gewählt werden.

i. Bundesdatenschutzgesetz

Das Bundesdatenschutzgesetz (BDSG) reguliert die Erfassung und Verwendung personenbezogener Daten sowie die Verarbeitung dieser Daten, darunter insbesondere:

- Aufzeichnung
- Änderung
- Übermittlung
- Blockierung
- Löschung[19]

Ein Großteil der Daten von Mitarbeitern, die ein Unternehmen unter Umständen für eine Untersuchung oder einen Rechtsstreit benötigt, sind in gewisser Hinsicht gemäß dem Bundesdatenschutzgesetz geschützt, da sie als personenbezogene Daten gelten. In der Tat definiert das BDSG personenbezogene Daten als „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)“.[20]

Von allen EU-Mitgliedstaaten hat Deutschland wohl die strengsten Datenschutzbeschränkungen und gibt den Angestellten starke Rechte über ihre persönlichen Daten. Die Erfassung und Verarbeitung von Mitarbeiterdaten darf nur unter bestimmten Umständen erfolgen und sollte der Vorgabe entsprechen, so wenig personenbezogene Daten wie möglich zu erfassen.[21] Dies steht im Einklang mit dem allgemeinen europäischen Ansatz des Abwägens bei der Suche nach der am wenigsten eingriffsintensiven praktikablen Vorgehensweise. Die Standards, die ein Unternehmen einhalten muss, um Daten von Mitarbeitern zu

erfassen oder zu verarbeiten, hängen sehr stark von der vom Unternehmen vorgesehenen Nutzung dieser Daten ab. Es gibt zum Beispiel unterschiedliche Kriterien zur Verwendung von Mitarbeiterdaten zu gewerblichen Zwecken,[22] zur Datenübermittlung,[23] zur Marktforschung[24] oder zu beschäftigungsrelevanten Zwecken.[25] Unabhängig von der vorgesehenen Nutzung muss es ein Gleichgewicht zwischen dem rechtmäßigen Geschäftsinteresse des Unternehmens und dem Schutz der Privatsphäre der betreffenden Mitarbeiter geben.[26]

Das BDSG schreibt zudem die Pflicht vor, Mitarbeiter zu benachrichtigen, wenn personenbezogene Daten unter bestimmten Umständen erfasst werden. Im Allgemeinen besteht die Benachrichtigungspflicht, wenn die Daten des Mitarbeiters ohne dessen Wissen verwendet werden.[27] Es gibt jedoch viele Ausnahmen, die, wenn zutreffend, die Unternehmen von der Benachrichtigung der Mitarbeiter ausnehmen.[28] Für Unternehmen kann auch eine Benachrichtigungspflicht gegenüber zuständigen Aufsichtsbehörden bestehen, wenn es Verstöße hinsichtlich der Erfassung, Verarbeitung oder Verwendung der Mitarbeiterdaten gegeben hat.[29]

Schließlich unterscheidet das BDSG zwischen strafrechtlichen Verletzungen und Verwaltungsvergehen. Verwaltungsvergehen können mit Geldbußen von bis zu 300.000 € bestraft werden.[30] Zudem können strafrechtliche Verletzungen strafrechtlich verfolgt werden, wenn der Mitarbeiter, das Unternehmen, der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit oder die Aufsichtsbehörde Beschwerde einreicht.[31] Neben den Geldbußen müssen Unternehmen unter Umständen Maßnahmen zur Berichtigung, Löschung oder Blockierung fehlerhafter personenbezogener Daten ergreifen, wenn ein Verstoß festgestellt wird.[32]

ii. Landesrechtliche Datenschutzgesetze

Der Datenschutz wird auch auf Ebene der Bundesländer geregelt. Auch wenn alle 16 Bundesländer Gesetze beibehalten, die das Bundesdatenschutzgesetz widerspiegeln,[33] können die einzelnen Datenschutzgesetze je nach Bundesland leicht voneinander abweichen. Generell lässt sich sagen, dass der Ansatz der Datenschutzbehörden in Bayern – mit der Landeshauptstadt München, Sitz vieler Konzernzentralen – gegenüber betrieblichen Herausforderungen bei der Datenerfassung üblicherweise offener zu sein scheint als die mehr landwirtschaftlich geprägten Bundesländer, z. B. Schleswig-Holstein.

Die Summe der Schadensersatzzahlungen beträgt in Bayern zum Beispiel nur 125.000 €,[34] kann in Hessen jedoch bis zu 250.000 € erreichen.[35] In vielerlei Hinsicht sind die landesrechtlichen Datenschutzgesetze jedoch einheitlich. Jede gesetzgebende Körperschaft der Bundesländer ernennt einen eigenen Landesbeauftragten für den Datenschutz. Der Landesbeauftragte handelt unabhängig und steht unter der Aufsicht des Landtagspräsidenten.[36] Der Bundesbeauftragte beaufsichtigt darüber hinaus Privatunternehmen innerhalb seiner Zuständigkeit, um die Einhaltung des Bundesdatenschutzgesetzes sicherzustellen.[37] Ebenso wie das Bundesgesetz schreiben die meisten landesrechtlichen Datenschutzgesetze eine Benachrichtigung und die Einholung der Zustimmung vor, bevor die Verarbeitung der personenbezogenen Daten vorgenommen werden kann.

iii. Einhaltung von bundesrechtlichen und landesrechtlichen Datenschutzgesetzen

Die Einhaltung der deutschen Datenschutzregelungen wird erreicht durch die Selbstüberwachung innerhalb des Unternehmens und durch die externe Aufsicht durch Bundes- und Landesbeamte. Bundes- und Landesbeauftragte für den Datenschutz sind dafür verantwortlich, dass Unternehmen die Gesetze befolgen. Diese Beauftragten sind ermächtigt, Verstöße zu untersuchen, und können zudem Prüfungen durchführen, damit sichergestellt ist, dass die organisatorischen und technischen Sicherheitsmaßnahmen des Unternehmens dem geltenden Datenschutzgesetz ausreichend gerecht werden.[38] Genau genommen müssen Landesbeauftragte regelmäßig Tätigkeitsberichte (mindestens alle 2 Jahre) veröffentlichen.[39] Wird der Rechtsverstoß eines Unternehmens festgestellt, sind die Beauftragten berechtigt, die betreffenden Mitarbeiter, Strafverfolgungsbehörden und sogar Gewerbeaufsichtsämter über diesen zu benachrichtigen, um Maßnahmen nach Gewerberecht einzuleiten.[40] Die Beauftragten sind außerdem dazu berechtigt, Geldbußen zu verhängen, Unternehmen dazu aufzufordern, Verstöße zu beseitigen, und sogar die Erfassung, Verarbeitung oder Verwendung von Mitarbeiterdaten vollständig zu untersagen.[41]

Unternehmen sind zudem zur Selbstkontrolle verpflichtet, damit ihre eigene interne Einhaltung der Vorgaben gewährleistet ist. Jedes Unternehmen muss zur Überwachung seiner Praktiken einen Datenschutzbeauftragten benennen. Der Datenschutzbeauftragte untersteht direkt der

Unternehmensführung und ist für die Einhaltung der geltenden Datenschutzgesetze und Vertretung des Unternehmens gegenüber externen Regierungsbehörden verantwortlich, die die Datenschutzgesetze auf Bundes- und Landesebene umsetzen.[42] Der Datenschutzbeauftragte ist außerdem dafür zuständig, dass Mängel der Datenschutzregelungen des Unternehmens behoben werden. Mitarbeiter, deren Daten gezielt erfasst werden, können den Datenschutzbeauftragten bei Bedenken jederzeit kontaktieren.[43]

IV. Erzielung der Zustimmung des Betriebsrats zum Erfassen von Mitarbeiterdaten

Zur Durchführung einer digitalen Suche und Anwendung einer Erfassungstechnologie auf unternehmensweiter Basis ist es erforderlich, die Zustimmung des Betriebsrats des Unternehmens zu erhalten. In der praktischen Umsetzung heißt dies, dass vorab ein Treffen mit dem Betriebsrat erforderlich ist, bei dem die Notwendigkeit der gewünschten Technologie dargelegt sowie aufgezeigt wird, wie die Technologie funktioniert und wie der Prozess zum Einsatz dieser Technologie so angepasst werden kann, dass der Eingriff in die Privatsphäre der Mitarbeiter möglichst gering ist.

Betriebsräte unterscheiden sich von Unternehmen zu Unternehmen, und jedes Unternehmen hat ein eigenes Verhältnis zu seinem Betriebsrat, das bei der Art der bestmöglichen Vorstellung dieses Themas zu berücksichtigen ist. Empfohlen wird, alle verfügbaren Informationen zur Dynamik dieses Verhältnisses vor der Präsentation zusammenzutragen. Aufgrund der Befindlichkeiten zu Datenschutzfragen in Deutschland – und der Tatsache, dass Datenschutz als Grundrecht gilt – trifft man unter Umständen auf anfängliche Skepsis bei Betriebsratsmitgliedern zum Prozess der Durchsuchung und Erfassung von E-Mails oder anderen potenziellen personenbezogenen Daten von Mitarbeitern. Um dieser anfänglichen Skepsis entgegenzuwirken, muss gezeigt werden, wie eine unternehmensweite digitale Such- und Erfassungstechnologie, z. B. EnCase® eDiscovery oder EnCase® Enterprise, als Teil des Prozesses eingesetzt werden können, der Schutz vor Missbrauch der Privatsphäre der Mitarbeiter bietet.

Teilweise werden Unternehmens- oder Mitarbeiterdaten durchsucht, um Fehlverhalten aufzudecken, und teilweise werden diese Daten durchsucht, um nach Kreditkarteninformationen von Mitarbeitern oder Kunden zu suchen und vor Hackern zu schützen. Es lohnt sich, darauf hinzuweisen, dass Datenerfassungen durch unternehmensinterne Untersuchungen in größeren Unternehmen in Deutschland zu einem festen Bestandteil geworden sind. In den vergangenen Jahren gab es in Deutschland eine Entwicklung dahingehend, dass Unternehmen stärker bei Regierungsermittlungen mitgearbeitet haben, insbesondere in Form von Selbstanzeigen bei Hinweisen auf Verstöße infolge interner Untersuchungen. Linde AG, ein Industriegasproduzent und Ingenieurunternehmen, konnte 2011 beispielsweise Korruptionsvorwürfe bereits zu einem frühen Zeitpunkt der Ermittlungen und vor der Anklage unauffällig klären, indem eine interne Untersuchung mit Unterstützung eines externen Anwalts durchgeführt und die Staatsanwaltschaft in München aktiv über Bestechungszahlungen informiert wurde, die Berater im Namen von Linde vorgenommen hatten.[44] Die Zahl deutscher Unternehmen hat zugenommen, die angesichts behördlicher Ermittlungen öffentlich erklären, dass sie interne Untersuchungen durchgeführt haben und mit den Behörden uneingeschränkt zusammenarbeiten.[45] Diese Entwicklung wurde teilweise durch Bestimmungen von Antikorruptionsgesetzen begünstigt, z. B. das britische Anti-Bestechungsgesetz, das Selbstanzeigen bei größeren Korruptionsfällen belohnt, sowie eine Änderung des deutschen Strafrechts von 2009, die Geständnishandel zuließ, was sehr wahrscheinlich zu einer stärkeren Zusammenarbeit zwischen der Staatsanwaltschaft und den unter Anklage stehenden Mitarbeitern, und indirekt ihren Arbeitgebern, führen wird.[46]

Angesichts der Tatsache, dass deutsche Unternehmen zunehmendem Druck ausgesetzt sind sowie Anreize geschaffen wurden, diese internen Untersuchungen durchzuführen – und von der Weitergabe der Ergebnisse gegenüber den Behörden zu profitieren –, stellt sich die Frage, wie diese Daten am besten erfasst werden können, sodass die Privatsphäre der Mitarbeiter bestmöglich geschützt wird. Bei dieser Zusammenarbeit stellt der Datenschutz einen zentralen Aspekt dar, wobei besonderes Augenmerk auf die Sicherheitsmaßnahmen bei der Lieferung personenbezogener Daten an die Staatsanwaltschaft und der Einholung schriftlicher Genehmigungen bei der Staatsanwaltschaft gelegt wird, damit das angemessene Datenschutzniveau erreicht wird. All dies erfordert jedoch die Erfassung der Mitarbeiterdaten von deren Rechnern und dem Computernetzwerk des Unternehmens aus.

Es obliegt deshalb dem Betriebsrat, unter verschiedenen Optionen zur Erfassung von Unternehmens- und Mitarbeiterdaten einen Ansatz zu finden, der am wenigsten in die Privatsphäre der Mitarbeiter eingreift. Im Gegensatz zu alternativen Maßnahmen der Datenerfassung, wie der Erstellung eines vollständigen Datenträgerabbilds der Mitarbeiterlaptops, ermöglicht die EnCase-Technologie eine gezielte Durchsuchung und Erfassung und erfasst nur diejenigen E-Mails und Dokumente, die zum Suchkriterium passen, sodass die übrigen personenbezogenen Daten nicht angefasst werden. Die EnCase-Technologie überwacht keine Daten oder Kommunikation von Mitarbeitern. Anders ausgedrückt, wird mit dieser Technologie weder die Nutzung der Rechner durch die Mitarbeiter ständig überprüft noch eine Rückmeldung erstellt, wann E-Mails verschickt oder empfangen werden. Die Überwachung stellt eine besonders schwerwiegende Verletzung des Datenschutzes dar: Datenschutzgesetze und Regulierungsbehörden sehen diese daher sehr kritisch. Betriebsratsmitglieder könnten vermuten, dass eine Überwachung vorgeschlagen wird. Die EnCase-Technologie unterstützt keine Mitarbeiterüberwachung in diesem Sinne. Ganz im Gegenteil: Sie ermöglicht die gezielte Erfassung von Daten („anvisieren, zielen und schießen“) von speziell festgelegten Laptops, Arbeitsplatzrechnern oder Servern. Die Kommunikation oder andere Arbeiten auf dem Computer der Mitarbeiter werden nicht überwacht.

Nachfolgend aufgelistet sind weitere mögliche Gesprächspunkte für einen erfolgreichen Antrag auf Verwendung von EnCase Enterprise oder EnCase eDiscovery beim Betriebsrat:

- **Versuchen Sie, so zeitig wie möglich auf die Tagesordnung des Betriebsrats gesetzt zu werden.** Üblicherweise wird dies durch die Personalabteilung des Unternehmens vorgenommen, die mit dem Betriebsrat zusammenarbeitet. In einigen Fällen kann es Monate dauern, Teil der Tagesordnung für eine monatliche Besprechung zu werden.
- **Halten Sie Ihre Präsentation auf Deutsch.** Auch wenn es banal klingen mag, sollte darauf hingewiesen werden, dass auch wenn die Führungspersonen, die die Datenerfassung durchführen, englischsprachig sind, die Präsentation und Beantwortung von Fragen von einer deutschsprachigen Führungskraft durchgeführt werden sollten (die Präsentationsunterlagen sollten ebenfalls auf Deutsch erstellt sein). Gibt es eine Person, die erhebliche Verantwortung für die Erfassung trägt, aber kein Deutsch spricht, sollte sie ebenfalls an dem Treffen teilnehmen, um Respekt zu zeigen und um für schwierige Fragen zur Verfügung zu stehen.
- **Stellen Sie heraus, dass mithilfe der EnCase-Technologie die Erfassung persönlicher E-Mails oder Dokumente der Mitarbeiter vermieden werden kann.** Mit EnCase-Produkten durchforsten Ihre Erfassungsroutinen die Daten und speichern ausschließlich die E-Mails und elektronischen Dokumente, die exakten Suchkriterien, u. a. Stichwörtern und Dateitypen, entsprechen. Andere Dokumente, die die Suchkriterien nicht erfüllen, einschließlich privater personenbezogener Daten, werden nicht erfasst.
- **Sichern Sie zu, dass die erfassten Daten im Land bleiben.** Einige Betriebsräte sind beruhigt zu hören, dass die vorgeschlagenen Maßnahmen die Aufbewahrung von erfassten Daten für einen möglichst langen Zeitraum in Deutschland vorsehen. Mithilfe der EnCase-Produkte ist es möglich, erfasste Daten von jedem Standort des Netzwerks aus herunterzuladen, d. h., die Daten können an einem sicheren Ort innerhalb von Deutschland heruntergeladen werden, selbst wenn die Technologie außerhalb von Deutschland betrieben wird. Stellt der Standort des Betreibers der Technologie ein Problem dar, kann der EnCase Examiner (die Softwareanwendung, die von einem Laptop oder einem Arbeitsplatzrechner aus betrieben wird) einfach an einem Standort in Deutschland, sofern nicht bereits vorhanden, eingesetzt werden.
- **Die EnCase-Technologie kann so konfiguriert werden, dass Mitarbeiterdaten nicht außerhalb von Europa übertragen werden.** Die Datenschutzgesetze der EU lassen Übertragungen zu anderen Rechtssystemen der Europäischen Union zu, schränken aber die meisten Übertragungen außerhalb von Europa ein. EnCase Enterprise und EnCase eDiscovery können so konfiguriert werden, dass das Durchsuchen von Daten europäischer Mitarbeiter von außerhalb Europas nicht möglich ist und die erfassten Daten nicht an Standorte außerhalb Europas übertragen werden.

- **Vorhandene Untersuchungsrichtlinien, die bereits vom Betriebsrat genehmigt wurden, können in Kraft bleiben.** Richtlinien der Personalabteilung zur Untersuchung von möglichem Fehlverhalten von Mitarbeitern beispielsweise, denen der Betriebsrat vor Kurzem zugestimmt hat, werden durch den Einsatz von EnCase eDiscovery oder EnCase Enterprise nicht berührt. Hierzu zählen auch die Zusicherungen, dass die erfassten Daten direkt zur Personalabteilung des Unternehmens geleitet und auch sonst wie immer verarbeitet werden.
- **Gestatten Sie Mitarbeitern, einen persönlichen Ordner anzulegen.** Erstellen Mitarbeiter in ihrer Dateistruktur des Rechners einen Ordner mit einem festgelegten Ordnernamen, in dem sie ihre gesamten personenbezogenen Daten ablegen können, kann das Suchkriterium der EnCase-Produkte so konfiguriert werden, dass dieser Ordner nicht durchsucht wird und diese Daten somit weder verarbeitet noch erfasst werden.
- **Durchsuchungen können nach Dateityp eingeschränkt werden.** Mitarbeiter können bei bestimmten Dateitypen, die für das Unternehmen vermutlich nicht von Interesse sind (z. B. persönliche Fotos), sehr empfindlich reagieren. Mit der EnCase-Technologie können auch diese Dateitypen von der Durchsuchung ausgeschlossen werden.
- **Transparenz.** EnCase Enterprise und EnCase eDiscovery verfügen über eine Prüffunktion, mit der festgelegte Personen im Unternehmensnetzwerk einen Echtzeitbericht zu allen Abfragen und Erfassungen erhalten können, die mit dieser Technologie vorgenommen wurden. Diese Prüffunktionen können festgelegten Mitarbeitern der Rechts- oder Personalabteilung, dem Datenschutzbeauftragten des Unternehmens oder Mitgliedern des Betriebsrats selbst angeboten werden.

V. Schlussfolgerung

Die in diesem Whitepaper unterbreiteten Vorschläge stammen aus Gesprächen mit Experten aus den Bereichen Recht und Informationssicherheit von einem guten Dutzend weltweiter Unternehmen. Diese Vorschläge wurden bei ihren deutschen Betriebsräten erfolgreich angewendet, um die Zustimmung zur Einführung von EnCase Enterprise oder EnCase eDiscovery zur Datenerfassung in Deutschland zu erhalten. Diese Betriebsräte kamen zu der Schlussfolgerung, dass der Einsatz der EnCase-Technologie, bei Verwendung innerhalb der engen Grenzen eines streng datensensiblen Prozesses, dem Unternehmen dabei hilft, die richtige Balance zwischen seinen rechtmäßigen Geschäftsinteressen bei gezielten digitalen Untersuchungen sowie den Datenschutzrechten der Mitarbeiter zu finden.

ANHANG I: Wichtige Akteure

Bundesbeauftragter für den Datenschutz:

Der Bundesbeauftragte für den Datenschutz wird vom Deutschen Bundestag für eine Amtszeit von 6 Jahren gewählt, ist bei der Ausübung seiner Tätigkeiten unabhängig und nur dem Gesetz unterworfen. Beim Aufdecken von Verstößen gegen das Bundesdatenschutzgesetz kann der Bundesbeauftragte für den Datenschutz einer Korrektur widersprechen oder diese verlangen. Der Beauftragte wird bei seinen Tätigkeiten von der Datenschutzkommission unterstützt – einer Gruppe von zehn Abgeordneten, die dem Beauftragten als Beratungsgremium zur Seite stehen.

Landesbeauftragte für den Datenschutz:
Ganz ähnlich wie beim Bundesbeauftragten für den Datenschutz wählt auch jedes Landesparlament einen Beauftragten für den Datenschutz, um die Einhaltung des landesrechtlichen Datenschutzgesetzes zu überwachen.

Datenschutzbeauftragter des Unternehmens:
Unternehmen benennen interne Datenschutzbeauftragte. Diese Beauftragten sind (1) verantwortlich für die Kontrolle von Daten, um unbefugten Zugriff oder die Eingabe personenbezogener Daten zu verhindern, müssen (2) sicherstellen, dass die Personen, die Zugriff auf das Datenverarbeitungssystem haben, nur auf die Daten zugreifen, für die sie eine Zugriffsberechtigung haben, (3) dass Daten ohne entsprechende Genehmigung zu keinem Zeitpunkt erfasst, verändert oder entfernt werden können, (4) dass die Veränderung von Daten dokumentiert werden kann, (5) dass bei Offenlegung von Daten dies dokumentiert wird, (6) dass der Bevollmächtigte zur Verarbeitung nur Daten gemäß Unternehmensanweisungen erfasst und diese Daten vor der Löschung geschützt werden.

Betriebsräte:
Betriebsräte können in Unternehmen gegründet werden, die 5 oder mehr wählbare Angestellte aufweisen. Ein Betriebsrat ist eine Form der Demokratie am Arbeitsplatz, wobei von Angestellten gewählte Vertreter Managementfunktionen erhalten. Betriebsräte haben das Recht, bei Angelegenheiten, die die Unternehmensstruktur betreffen, Personalentscheidungen, Richtlinien zum Arbeitsplatz und individuellem Verhalten innerhalb des Unternehmens mitzubestimmen. Dies bedeutet, dass jede vorgeschlagene Richtlinie zunächst vom Betriebsrat genehmigt werden muss, um im Unternehmen umgesetzt werden zu können.

ANHANG II: Nützliche Links

EU-Richtlinie (englische Fassung):
http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML

Bundesdatenschutzgesetz (auf Englisch):
http://www.bfdi.bund.de/EN/DataProtectionActs/Artikel/BDSG_idFv01092009.pdf?__blob=publicationFile

Betriebsverfassungsgesetz (auf Englisch):
http://www.bmwi.de/English/Redaktion/Pdf/__Archiv/labour-law/works-constitution-act1,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf

Links zu ausgewählten landesrechtlichen Datenschutzgesetzen (sofern nicht anders angegeben, sind alle Dokumente auf Deutsch verfasst):
Baden-Württemberg:
http://www.zv.uni-wuerzburg.de/datenschutz/Gesetze/bayer_datenschutzgesetz.htm

Bayern:
http://byds.juris.de/byds/009_1.1_DSG_BY_1993_rahmen.html

Berlin:
http://www.datenschutz-berlin.de/content/Recht

Brandenburg:
http://www.lda.brandenburg.de/cms/detail.php?gsid=bb1.c.233960.de

Hamburg:
http://www.datenschutz-hamburg.de/

Hessen:
http://www.datenschutz.hessen.de/hdsg99.htm

Mecklenburg-Vorpommern:
http://www.lfd.m-v.de/datenschutz/rechtsgrundlagen/rechtsgrundlagen.html

Niedersachsen:
http://www.lfd.niedersachsen.de/portal/live.php?navigation_id=12908&_psmand=48

Nordrhein-Westfalen:
https://www.ldi.nrw.de/

Rheinland-Pfalz:
http://www.datenschutz.rlp.de/rgrundlagen/a1_5.html

Saarland:
http://sl.juris.de/cgi-bin/landesrecht.py?d=http://sl.juris.de/sl/DSG_SL_2007_rahmen.htm

Sachsen:
www.datenschutz.sachsen.de

Schleswig-Holstein (auf Englisch):
https://www.datenschutzzentrum.de/material/recht/ldsg-eng.htm

Thüringen:
http://www.thueringen.de/datenschutz/gesetze_rechtsvorschriften/thueringen/datenschutzgesetz/

FUSSNOTEN

1 Der Verfasser dieses Textes spricht Donna Salcedo, Rechtspraktikantin bei Reed Smith LLP, für ihre umfassende Unterstützung beim Schreiben dieses Whitepapers Dank und Anerkennung aus.

2 EnCase® eDiscovery ist eine elektronische Erkennungssoftware, die eine Reihe von Funktionen von der Sicherung und Erfassung bis zur Prüfung und Erstellung von Daten anbietet. EnCase® Enterprise ist eine Softwareplattform, mit der Unternehmen Daten von Servern und Arbeitsplatzrechnern netzwerkübergreifend ohne Störung des Geschäftsbetriebs eingrenzen, durchsuchen, erfassen, speichern und analysieren können. EnCase®-Technologie bezieht sich auf die Kernfunktionen, die sowohl bei EnCase® eDiscovery als auch bei EnCase® Enterprise vorhanden sind.

3 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

4 Bundesministerium für Wirtschaft und Technologie, Betriebsverfassungsgesetz, §1, http://www.bmwi.de/English/Redaktion/Pdf/__Archiv/labour-law/works-constitution-act1,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf

5 Id. §14(2).

6 Id. §14(5).

7 Id. §14(1).

8 Id. §21

9 Id. §15(2).

10 Ingebjörg Darsow, Implementation of Ethics Codes in Germany: The Wal-Mart Case, Universität Pompeu Fabra, (März 2005) abrufbar unter http://www.upf.edu/iuslabor/032005/art11.htm

11 Bundesministerium für Wirtschaft und Technologie, Betriebsverfassungsgesetz, §§ 80, 81, 85 und 89, http://www.bmwi.de/English/Redaktion/Pdf/__Archiv/labour-law/works-constitution-act1,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf

12 Id. §33.

13 Id. §77.

14 Id. §77(5).

15 Id. §76.

16 Id. §96.

17 Am 25. Januar 2012 schlug die Europäische Kommission eine umfassende Reform der EU-Richtlinie vor, die ein einheitliches Gesetz für alle Mitgliedstaaten zur Folge haben würde. Der Vorschlag ist noch anhängig. Selbst wenn der Reform zugestimmt wird, kann es bis zu 2 Jahre dauern, bis die Mitgliedstaaten das neue Gesetz umgesetzt haben. Zum Zeitpunkt der Erstellung des vorliegenden Dokuments behält jedoch jeder Mitgliedstaat seine eigene Gesetzgebung zur Befolgung der allgemeinen Grundsätze der EU-Richtlinie bei. Siehe Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Allgemeine Datenschutzbestimmungen), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52012PC0010:en:NOT

18 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995, Abschnitt II, Art. 7(f), Amtsblatt der Europäischen Gemeinschaften 1995, Nr. L 281/31 [die EU-Richtlinie] abrufbar unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML

19 Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Bundesdatenschutzgesetz, §§ 1, 3(3), 3(4) und 3(5), http://www.bfdi.bund.de/EN/DataProtectionActs/Artikel/BDSG_idFv01092009.pdf?__blob=publicationFile

20 Id. §3(1).

21 Id. §3a.

22 Id. §28(1).

23 Id. §§ 28a, 29 und 30.

24 Id. §30a.

25 Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Bundesdatenschutzgesetz, § 32, http://www.bfdi.bund.de/EN/DataProtectionActs/Artikel/BDSG_idFv01092009.pdf?__blob=publicationFile

26 Id. §35(5).

27 Id. §33(1).

28 Id. §33(2).

29 Id. §42(a).

30 Id. §43(3).

31 Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Bundesdatenschutzgesetz, § 44, http://www.bfdi.bund.de/EN/DataProtectionActs/Artikel/BDSG_idFv01092009.pdf?__blob=publicationFile

32 Id. §35.

33 Siehe Sidebar mit der Überschrift „Nützliche Links“ für Links zu verschiedenen landesrechtlichen Datenschutzgesetzen.

34 Bayerisches Datenschutzgesetz, § 14, http://translate.google.com/translate?hl=en&sl=de&u=http://byds.juris.de/byds/009_1.1_DSG_BY_1993_rahmen.html&prev=/search%3Fq%3Dhttp://byds.juris.de/byds/009_1.1_DSG_BY_1993_rahmen.html%26hl%3Den%26client%3Dsafari%26tbo%3Dd%26rls%3Den&sa=X&ei=nEUZUeKMEvGX0gGCl4GQBg&ved=0CDgQ7gEwAA

35 Hessisches Datenschutzgesetz, § 20, http://translate.google.com/translate?hl=en&sl=de&tl=en&u=http%3A%2F%2Fwww.datenschutz.hessen.de%2Fhdsg99.htm

36 Siehe z. B. Bayerische Verfassung, Art. §33(a), abrufbar unter www.taxi-muenchen-online.de/programme/bavarian_const.pdf, siehe auch Sächsisches Datenschutzgesetz, §22.

37 Datenschutzgesetz von Sachsen-Anhalt, §22.

38 Bundesdatenschutzgesetz, Fußnote 16, bei §38(4).

39 Id. §38(1).

40 Id.

41 Id. §38(5).

42 Id. §4(f).

43 Id. §4(f)(5).

44 Gibson Dunn 2011 Year-End German Law Update „Compliance – Recent Cases Show Different Ways to Successfully Settle Investigations“ Punkt 9, http://www.gibsondunn.com/publications/pages/2011YearEndGermanLawUpdate.aspx.

45 Siemens AG und MAN SE arbeiteten in den vergangenen Jahren mit der Staatsanwaltschaft zusammen und tauschten Informationen zu Bestechungs- und Korruptionsvorwürfen aus, die diese Unternehmen aufgrund interner Untersuchungen erhielten. ICID Review, Frühjahr 2010 S. 11. Die Fresenius Medical Care AG gab gleichfalls im August 2012 bekannt, dass das Unternehmen eine interne Untersuchung zu möglichen Verstößen des US-amerikanischen Gesetzes zur Korruptionsbekämpfung (Foreign Corrupt Practices Act) eingeleitet hat (siehe http://blogs.wsj.com/corruption-currents/2012/08/03/german-dialysis-maker-opens-fcpa-probe/). ThyssenKrupp AG gab im Dezember 2012 bekannt, dass ein Vorstandsmitglied aufgrund laufender interner und öffentlicher Ermittlungen zu luxuriösen Geschäftsreisen um Suspendierung gebeten hat (siehe http://m.foxbusiness.com/quickPage.html?page=19453&content=84412818&pageNum=-1). Trotz öffentlicher Erklärungen der Deutschen Bank, dass das Unternehmen uneingeschränkt mit Behörden zusammenarbeitet, wurde es am 12. Dezember 2012 Ziel der größten Hausdurchsuchung in der deutschen Geschichte, als mehr als 500 Strafverfolger und Polizeibeamte die Büroräume und Wohnorte der Mitarbeiter in Frankfurt/Main, Berlin und Düsseldorf durchsuchten. Die Staatsanwaltschaft sagte, dass gegen 25 Bankangestellte wegen Verdachts auf schwere Steuerhinterziehung, Geldwäsche und Behinderung der Justiz ermittelt wurde. Der Spiegel, „Head Office Raided in Tax Probe: Deutsche Bank CEO Under Investigation“, 12. Dezember 2012, http://www.spiegel.de/international/business/deutsche-bank-co-ceo-juergen-fitschen-under-investigation-in-tax-probe-a-872563.html Die Staatsanwaltschaft behauptetet, dass die Deutsche Bank auf die vorherigen Informationsanfragen der Behörden nicht angemessen reagiert hat. Gibson Dunn 2012 Year-End German Law Update „Compliance - Public Investigations on the Rise“ S. 22, http://www.gibsondunn.com/publications/pages/2012YearEnd-GermanLaw-Update.aspx

46 Gesetz zur Regelung der Verständigung im Strafverfahren, BGBl. I.S. 2353; siehe auch ICID-Review, Frühjahr 2010 „Cooperation with German Investigation Authorities“ S. 1, 10-12.

Zu Patrick J. Burke

Patrick J. Burke ist als Anwalt im New Yorker Büro von Reed Smith LLP tätig (pburke@reedsmith.com, Tel.: 212-549.0313) und arbeitet dabei mit der Archivierungs- und E-Discovery-Gruppe des Unternehmens und Klienten in den Bereichen elektronische Erkennung, Datenschutz, Archivverwaltung, Information Governance und Cyber-Sicherheit zusammen. Er ist als Experte für das Recht auf Privatsphäre (Certified Information Privacy Professional) für europäischen Datenschutz (CIPP/E) zertifiziert. Patrick J. Burke ist außerordentlicher Professor an der juristischen Fakultät Benjamin N. Cardozo, wo er zu den Themen elektronische Erkennung, digitale Beweisführung und Computerkriminaltechnik lehrt.

Er dankt seiner Rechtspraktikantin bei Reed Smith, Donna Salcedo, für ihre wertvollen Beiträge zu diesem Whitepaper.

Unsere Kunden

Die Kunden von Guidance Software sind Unternehmen und staatliche Einrichtungen aus den verschiedensten Branchen, z. B. Finanz- und Versicherungswesen, Technologie, Defense Contracting, Pharmaindustrie, Herstellung und Einzelhandel. Zu unseren repräsentativen Kunden zählen Allstate, Chevron, FBI, Ford, General Electric, Honeywell, NATO, Northrop Grumman, Pfizer, SEC, UnitedHealth Group und Viacom.

Über Guidance Software (NASDAQ: GUID)

Guidance Software ist weltweit als Branchenführer bei digitalen Investigativlösungen anerkannt. Die EnCase® Enterprise-Plattform wird von zahlreichen Regierungsbehörden, mehr als 65 Prozent der *Fortune* 100-Unternehmen und mehr als 40 Prozent der *Fortune* 500-Unternehmen eingesetzt, um digitale Untersuchungen auf Servern, Laptops, Desktopgeräten und mobilen Geräten durchzuführen. Aufgebaut auf der EnCase Enterprise-Plattform werden die marktführenden Lösungen für elektronische Erkennung und Cyber-Sicherheit EnCase® eDiscovery und EnCase® Cybersecurity angeboten, mit denen Unternehmen auf Auskunftsersuchen bei Streitsachen reagieren, Erkennung sensibler Daten zur Einhaltung von Verpflichtungen und die Durchführung einer schneller und umfassenden Reaktion auf sicherheitsrelevante Ereignisse vornehmen können. Weitere Informationen zu Guidance Software erhalten Sie unter www.encase.com.

Weitere Informationen zu Guidance Software erhalten Sie unter www.encase.com.