Obtaining German Works Council Approval to Collect Employee E-Mail and Electronic Documents Using EnCase® Enterprise and EnCase® eDiscovery

By Patrick Burke
Counsel, Reed Smith LLP
pburke@reedsmith.com[1]

ReedSmith

I. Executive Summary

German companies sometimes are required to collect data for legitimate business purposes, including for compliance, to investigate malfeasance, for adjudication of claims and to protect personal data of customers from misuse. Companies that seek to employ EnCase® Enterprise or EnCase® eDiscovery[2] to search and collect German employees' e-mails and electronic documents face a critical requirement: obtaining permission from their companies' works councils in Germany. German works councils have a well-earned reputation as rigorous guardians of employee privacy rights, sometimes rejecting corporate efforts to search through employee data, invoking the rights and protections afforded German employees pursuant to the 1995 European Union Data Protection Directive[3] as well as German federal and state data protection laws implementing the Directive.

It is not uncommon, however, for German works councils to approve data collection approaches that include reasonable safeguards of employee privacy. In fact, the European data protection laws recognize that there should be a balance between the employees' fundamental human right to privacy versus the organization's legitimate business interests and legal obligations. This author has been involved in a number of successful requests to German works councils. The key to that success is to make a well-researched and sensitive presentation to the works council, and to offer a collection methodology that includes protections for employees' rights. EnCase® products can assist in this defensible methodology.

This white paper will address the following:

- What is a German works council and how does it function?
- What is the German data protection regime upon which a works council can base its objections?
- What steps can a company take to maximize the ability for EnCase® data collections to be approved by a German works council?

II. The German Works Councils

German works councils have been an integral part of German business and industry since the early 20th century. The first works council provision was enacted following World War I and has existed in various forms ever since. The existing law is enshrined in the Works Constitution Act of 1972 (Betriebsverfassungsgesetz) and applies to private enterprises with more than five permanent employees of voting age.[4]

Works councils are established through democratic processes. Candidates for works councils must secure a certain number of signatures from their fellow employees to be eligible for election.[5] Trade unions may also nominate candidates for election, but cannot compel their members to vote a specific way.[6] Works council members are elected directly by company employees through a secret ballot, though employees are not required to vote.[7] Elected members generally serve for four years.[8] The size of a works council depends on the number of employees within a company and must proportionately represent certain types of employees, like women.[9]

Under the Works Constitution Act, works councils have the right to co-determine matters affecting company structure, personnel decisions, and policies regulating workplace and individual conduct within the company.[10] The rights of a works council can be categorized as follows:

- **Information:** The right to information regarding the implementation or change of practices or policies at the company. If necessary, the employer must provide documentation to that effect.
- **Consultation and Cooperation:** The right to consult and cooperate with management to jointly discuss and develop the topic at issue.
- **Veto:** The right to block certain management decisions.

The employer is required to keep the works council fully informed on matters relating to operations and personnel planning so that the council can participate in drafting company policy.[11] Through this cooperation with the works council, management avoids potential disputes and raises relevant concerns or makes suggestions. Works council resolutions require a quorum of fifty percent and resolutions are adopted by simple majority unless otherwise required by law.[12] Works councils and management may, formally or informally, enter into valid and binding agreements.[13] Formal agreements are immediately binding on employers and employees, and informal agreements generally require additional steps, such as the amendment of an employee contract. The works council may only enter into "works bargaining agreements" in those areas of business operation where the Works Constitution Act confers rights of participation. Collective bargaining agreements between employer associations and trade unions have absolute priority over works bargaining agreements, even if the latter are more favorable to the workforce.[14]

In the event that disputes between works council and management cannot be resolved amicably, the parties may be assisted by the "conciliation board," a body with arbitration and mediation duties.[15] Assuming both parties agree to be bound by its decision beforehand, the conciliation board's ruling is final and binding and is appealable only on the grounds that the board has violated general principles of law.[16]

III. German Data Protection

When works councils assert their right to approve or disapprove employee data collection methodologies, they are in part invoking the employees' rights pursuant to European Union (EU) law, German federal law, and the data protection laws of their home states. Though all EU member states must meet the guidelines of the EU Directive, they are free to implement individual legislation within their states in order to reach these guidelines.[17]

The EU Data Protection Directive authorizes a balancing of legitimate business interests of the company against the employees' right to privacy.[18] Best practices indicate that this balance is best met when the means of "processing" data is the least intrusive practicable approach.

i. Federal Data Protection Act (Bundesdatenschutzgesetz)

Germany's Federal Data Protection Act (Bundesdatenschutzgesetz or BDSG) regulates the collection and use of personal data as well as the processing of such data, which includes specifically:

- Recording
- Alteration
- Transfer
- Blocking
- Deletion[19]

Much of the data held by employees that a company may require for an investigation or litigation will be protected under Germany's federal data protection law in some respect as it will be deemed "personal data." In fact, the BDSG defines personal data as "any information concerning the personal or material circumstances of an identified or identifiable natural person ('data subject')."[20]

Of the EU member states, Germany has some of the most stringent data privacy restrictions, giving employees strong rights over their personal data. Collection and processing of employee data can only occur under certain circumstances and should be in accordance with the aim to collect as little personal data as possible.[21] This is consistent with the general European balancing approach seeking the least intrusive practicable approach. The standards a company must meet in order to collect or process employee data depend heavily on the company's intent for the use of such data. For example, there are different criteria for using employee data to pursue commercial purposes,[22] transferring,[23] market research,[24] or employment-related purposes.[25] Regardless of the intended use, there must ultimately be a balance between the legitimate

business purposes of the company and the privacy interests of affected employees.[26]

The BDSG also imposes a duty to notify employees when personal data has been collected under certain circumstances. Generally, a duty to notify exists when the employee data is used without the employee's knowledge.[27] However, there are many exceptions that, when met, excuse companies from notifying employees.[28] Companies may also have a duty to notify the appropriate supervising authorities if there have been any violations with respect to the collection, processing, or use of an employee's data.[29]

Lastly, the BDSG differentiates between criminal and administrative violations of the law. Administrative violations may be punishable by a fine of up to €300,000,[30] while criminal violations may be prosecuted when complaints are filed by the employee, the company, the Federal Commissioner for Data Protection and Freedom of Information, or the supervisory authority.[31] In addition to fines, companies may also need to take steps to rectify, erase, or block inaccurate personal data if a violation is found.[32]

ii. State Data Protection Laws

Data protection is also regulated on the state level. Although all sixteen states of Germany maintain laws that mirror the Federal Data Protection Act,[33] each data protection law may be slightly different depending on the state. As a rule of thumb, the approach of data protection authorities in Bavaria –home to corporate headquarters-rich Munich – generally seems to be more open-minded toward corporate challenges in data collection than those in more agricultural states such as Schleswig-Holstein.

For example, damages in Bavaria may only reach €125,000,[34] while in Hesse they may reach up to €250,000.[35] The state data protection laws are, however, uniform in many respects. Each state legislative body appoints its own State Commissioner for Data Protection. The State Commissioner operates independently and is supervised by the President of the state legislature.[36] The State Commissioner also oversees private organizations within its jurisdiction to ensure compliance with the state data protection law.[37] Like the Federal Act, most state data protection laws provide for notification and the obtainment of consent before the processing of personal data can take place.

iii. Compliance with Federal and State Data Protection Laws

Compliance with the German data protection regime is achieved through self-monitoring within the company and external oversight by federal and state officials. Federal and state data protection commissioners are responsible for ensuring that companies comply with the law. These commissioners are empowered to investigate violations and may also perform audits to ensure that a company's organizational and technological safeguards sufficiently comply with the applicable data protection law.[38] In fact, federal commissioners must publish activity reports regularly and at least every two years.[39] If companies are found to be in violation of the law, commissioners are authorized to notify affected employees, the bodies responsible for prosecution or punishment, and even trade supervisory authorities in order to initiate measures under trade law.[40] Commissioners are also authorized to impose fines, order companies to remedy violations, and even prohibit collection, processing, or use of employee data entirely.[41]

Companies are also required to self-regulate to ensure their own internal compliance; each company is required to appoint a Data Protection Officer to monitor its practices. The Data Protection Officer reports directly to corporate management and is responsible for ensuring compliance with applicable data protection laws and representing the company to the external government agencies that enforce the data protection laws at the state and federal levels.[42] The Data Protection Officer is also tasked with ensuring that deficiencies in a company's data protection regime are rectified. Employees whose data is targeted may approach the data protection officer any time they have concerns.[43]

IV. Securing Works Council Approval to Collect Employee Data

In order to implement any digital search and collection technology on an enterprise-wide basis, it is necessary to secure the approval of the organization's works council. On a practical level, this means going before a meeting of the works council and outlining the need for such technology, how the technology works, and how the process around the use of that technology will be tailored to minimize intrusion on employee privacy.

Works councils are different in every organization, and each organization has its own relationship with its works council that will affect how best to present on this topic. It is advisable to gather any information available on the dynamic of that relationship in advance of your presentation. Due to the sensitivities around privacy in Germany – and the fact that data privacy is deemed a fundamental human right -- one may expect to encounter initial skepticism from works council members about any process that involves search and collection of employees' e-mails or other potentially personal data. To counter this initial skepticism, one must show how an enterprise-wide digital search and collection technology – such as EnCase® eDiscovery or EnCase® Enterprise –can be used as part of a process that offers safeguards against abuse of employees' privacy rights.

Sometimes corporate and employee data is searched to root out wrongdoing, and sometimes it is searched to locate and protect employee or customer credit card information from hackers. It is worthwhile to make the point that corporate internal investigations increasingly have made data collection a fact of life at major German corporations. The last few years have seen a trend in Germany for corporations to make greater efforts to cooperate with government investigations, in particular through self-disclosures of evidence of wrongdoing following internal investigations. For example, in 2011 Linde AG, an industrial gas producer and engineering company, was able quietly to resolve corruption charges in the early investigatory and pre-indictment stage, after it carried out an internal investigation with assistance of outside counsel and proactively informed Munich prosecutors about bribe payments made by consultants acting on Linde's behalf.[44] Increasingly German companies facing government investigations publicly assert that they have conducted internal investigations and are fully cooperating with the authorities.[45] This trend is fueled in part by provisions in anti-corruption laws such as the UK Bribery Act which reward voluntary self-disclosure in major corruption incidences, and a 2009 change to German criminal law allowing for plea agreements that likely will lead to greater cooperation between prosecutors and employees facing charges and, indirectly, their employers.[46]

Given the fact that German corporations face increased pressure and incentives to conduct such internal investigations – and receive credit for sharing the results with authorities – the question has become how best to collect such data in a way that allows for the greatest possible safeguarding of employee privacy. Data protection is a key consideration in such cooperation, with attention given to safeguards on the delivery of personal data to the prosecutors – sometimes including anonymization of data provided to authorities and obtaining written agreements with the prosecutor to ensure the appropriate level of data protection. All of this, however, requires the collection of employees' data from the employees' computers and the company's computer network.

It therefore is the role of the works council to choose among different options for collection of corporate and employee data, to find an approach that is the least intrusive on employee privacy. Unlike alternative means of data collection, such as full-disk "imaging" of employee laptops, EnCase technology enables "surgically" targeted search and collection, capturing only those e-mails or documents responsive to search criteria, and leaving the remaining personal data untouched. EnCase technology does not "monitor" employees' data or communications. In other words, it does not continually check on employees' use of their computers or report back when emails are sent or received. As a practice, monitoring represents a very troubling version of privacy violation; privacy laws and

regulators frown on monitoring. Works council members may jump to the conclusion that monitoring is being proposed. EnCase technology does not enable employee monitoring as so understood. Rather, it enables surgically targeted – "point, aim, and shoot" – collection of data from specifically identified laptops, workstations or servers. It does not keep watch over employees' communications or other work on their computer.

The following are additional suggested talking points for successful works council applications for the use of EnCase Enterprise or EnCase eDiscovery:

- **Get on the works council agenda as early as possible.** Usually this is handled through the company's Human Resources department, which generally interfaces with the works council. In some cases, it may take months just to get onto the agenda for a monthly meeting.

- **Make your presentation in German.** This may sound obvious, but it's worth noting that even though the managers who run your data collection operations are English speakers, they should employ a German-speaking manager to make the presentation and field questions (the presentation materials used should be in German, as well). If there is a non-German speaking manager with significant collection responsibility, he or she should also attend, both as a sign of respect and to be available for tough questions.

- **Emphasize that EnCase technology can enable you to avoid collecting employee personal e-mail or documents.** With EnCase products, your collections will cull through the data and preserve only those e-mails and electronic documents that meet precise search criteria, including keywords and file types. Other documents that do not meet the search criteria – including private personal data – will be left behind.

- **Assure that the collections will be kept "in-country."** Some works councils are reassured when the proposed process calls for keeping all data collected within Germany as much and as long as possible. EnCase products allow for the collected data to be downloaded to any location on the network, which means it can be downloaded to a secure location within Germany even if the technology is being operated from outside Germany. If the location of the operator of the technology is an issue, an EnCase "examiner" (the software application operated from laptop or workstation) can easily be deployed to a location in Germany if not already there.

- **EnCase technology can be configured to prevent employee data from being transferred outside of Europe.** EU data protection laws permit transfers to other European Union jurisdictions, but restrict most transfers outside Europe. EnCase Enterprise and EnCase eDiscovery can be configured to prevent searches of European employee data from outside of Europe, and prevent the transfer of data collected to locations outside Europe.

- **Existing investigative policies already approved by the works council can remain in place.** For example, Human Resources policies relating to the investigation of potential employee wrongdoing previously approved by the works council will not be affected by the use of EnCase eDiscovery or EnCase Enterprise. This includes guarantees that any data collected would go directly to the company's Human Resources team and would otherwise be handled the same as always.

- **Permit employees to create a "personal folder."** If employees create a folder in their computer file structure with an agreed-upon folder name in which they can place all of their personal data, the search criteria of EnCase products can be configured to leave that folder unsearched, so that

none of that data will be processed or collected.

- **Ability to restrict searches by file type.** Employees can be sensitive about certain types of files that may not be of interest to the company – personal photographs, for instance. With EnCase technology, these file types can be excluded from search, as well.

- **Transparency.** EnCase Enterprise and EnCase eDiscovery provide an "audit" function by which any designated person(s) on the organization's network can be provided with a real-time report on all search and collection performed using the technology. These audit capabilities can be offered to designated legal or HR professionals, the company's data protection officer, or to members of the works council itself.

V. Conclusion

The suggestions provided in this white paper come from interviews with legal and information security professionals from more than half a dozen global organizations that have applied successfully to their German works councils for authority to implement EnCase Enterprise or EnCase eDiscovery for collection of data in Germany. These works councils concluded that the use of EnCase technology – when used within the confines of a rigorous privacy-conscious process – enables the organization to strike the correct balance between its legitimate business interest in targeted digital investigations and the privacy rights of its employees.

APPENDIX I: Key Players

Federal Data Protection Commissioner:

The Federal Data Protection Commissioner is elected by the German Parliament for a term of six years, is independent in the exercise of his duties and is subject only to the law. Upon discovering violations of the German Federal Data Protection Act, the Data Protection Commissioner may object and demand correction of the violation. The Commissioner is supported in his duties by the Data Protection Commission, a group of ten members of Parliament who serve as an advisory panel to the Commissioner.

State Data Protection Commissioners:
Much like the Federal Data Protection Commissioner, each state's Parliament elects a Data Protection Commissioner to monitor compliance with that state's Data Protection Act.

Company Data Protection Officer:
Companies appoint Data Protection Officers within their organizations. These officers are responsible for (1) controlling data by preventing unauthorized persons from accessing or entering personal data; (2) assuring that those who have access to the data processing system are only accessing the data they have authority to access; (3) assuring that at no point can data be collected, modified or removed without authorization; (4) assuring that the modification of data can be documented; (5) assuring that whenever data is disclosed, it is documented; (6) assuring that the processing agent is only collecting data in accordance with a business's instructions and that such data is protected from destruction.

Works Councils:
Works councils are required for companies that normally employ five or more eligible employees. A works council is a form of workplace democracy whereby representatives elected by employees are given management functions. Works councils have the right to co-determination in matters affecting organizational structure, personnel

decisions, and policies regulating workplace and individual conduct within the company. This means that any proposed policy must first be approved by the works council in order to be implemented by the company.

APPENDIX II: Useful Links

EU Directive (English version):
http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML

German Federal Data Protection Act (in English):
http://www.bfdi.bund.de/EN/DataProtectionActs/Artikel/BDSG_idFv01092009.pdf?__blob=publicationFile

Works Constitution Act (in English):
http://www.bmwi.de/English/Redaktion/Pdf/__Archiv/labour-law/works-constitution-act1,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf

Links to Selected German States' Data Protection Laws (unless otherwise noted, all documents in German):
Baden-Württemberg:
http://www.zv.uni-wuerzburg.de/datenschutz/Gesetze/bayer_datenschutzgesetz.htm

Bavaria:
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/

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

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

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

North Rhine-Westphalia:
https://www.ldi.nrw.de/

Rhineland-Palatinate:
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

Saxony:
www.datenschutz.sachsen.de

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

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

ENDNOTES

1 The author acknowledges and thanks Donna Salcedo, Law Intern, Reed Smith LLP, for her extensive assistance with the writing of this whitepaper.

2 EnCase® eDiscovery is an electronic discovery software offering a range of functionality from legal hold and collection through review and production. EnCase® Enterprise is a software platform that enables organizations to target, search, collect, preserve and analyze data from servers and workstations network-wide without disrupting business operations. EnCase® technology refers to the core functionality present in both EnCase® eDiscovery and EnCase® Enterprise.

3 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

4 Federal Ministry of Economics and Technology, Works Constitution Act (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. at §14(2).

6 Id. at §14(5).

7 Id. at §14(1).

8 Id. at §21

9 Id. at §15(2).

10 Ingebjörg Darsow, Implementation of Ethics Codes in Germany: The Wal-Mart Case, Universitat Pompeu Fabra, (March 2005) available at http://www.upf.edu/iuslabor/032005/art11.htm

11 Federal Ministry of Economics and Technology, Works Constitution Act (Betriebsverfassungsgesetz), §§ 80, 81, 85, and 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. at §33.

13 Id. at §77.

14 Id. at §77(5).

15 Id. at §76.

16 Id. at §96.

17 On January 25, 2012, the European Commission proposed a comprehensive reform of the EU Directive, which would create a single uniform law applicable to all member states. The proposal is still pending. Even if the reform is approved, member states may take up to two years to implement the new law. As of the time of writing this paper, however, each member state retains its own legislation effectuating the general tenets of the EU Directive. See Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52012PC0010:en:NOT

18 Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995, Section II, art. 7(f), Official Journal of the European Communities 1995, No. L 281/31 [the "EU Directive"] available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML

19 The Federal Commissioner for Data Protection and Freedom of Information, Federal Data Protection Act (Bundesdatenschutzgesetz,) §§ 1, 3(3), 3(4), and 3(5), http://www.bfdi.bund.de/EN/DataProtectionActs/Artikel/BDSG_idFv01092009.pdf?__blob=publicationFile

20 Id. at §3(1).

21 Id. at §3a.

22 Id. at §28(1).

23 Id. at §§ 28a, 29, and 30.

24 Id. at §30a.

25 The Federal Commissioner for Data Protection and Freedom of Information, Federal Data Protection Act (Bundesdatenschutzgesetz,) §32, http://www.bfdi.bund.de/EN/DataProtectionActs/Artikel/BDSG_idFv01092009.pdf?__blob=publicationFile

26 Id. at §35(5).

27 Id. at §33(1).

28 Id. at §33(2).

29 Id. at §42(a).

30 Id. at §43(3).

31 The Federal Commissioner for Data Protection and Freedom of Information, Federal Data Protection Act (Bundesdatenschutzgesetz,) §44, http://www.bfdi.bund.de/EN/DataProtectionActs/Artikel/BDSG_idFv01092009.pdf?__blob=publicationFile

32 Id. at §35.

33 See Sidebar titled "Useful Links" for links to various state data protection laws.

34 Bavarian Data Protection Act, Article 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 Hessian Data Protection Act, § 20, http://translate.google.com/translate?hl=en&sl=de&tl=en&u=http%3A%2F%2Fwww.datenschutz.hessen.de%2Fhdsg99.htm

36 See, e.g., Bavarian Constitution, Art. §33(a), available at www.taxi-muenchen-online.de/programme/bavarian_const.pdf, , see also Saxony Data Protection Act, §22.

37 Saxony-Anhalt Data Protection Act, §22.

38 Federal Data Protection Act, supra note 16, at §38(4).

39 Id. at §38(1).

40 Id.

41 Id. at §38(5).

42 Id. at §4(f).

43 Id. at §4(f)(5).

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

45 Both Siemens AG and MAN SE cooperated with prosecutors in recent years by sharing information about alleged bribery and corruption which these companies obtained through internal investigations. ICID Review, Spring 2010 at 11. Likewise, Fresenius Medical Care AG announced in August 2012 that it had begun an internal investigation into potential violations of the U.S. Foreign Corrupt Practices Act (see http://blogs.wsj.com/corruption-currents/2012/08/03/german-dialysis-maker-opens-fcpa-probe/) and ThyssenKrupp AG announced in December 2012 that an executive board member had asked to be suspended, pending internal and public investigations into luxury business trip expenses (see http://m.foxbusiness.com/quickPage.html?page=19453&content=84412818&pageNum=-1). Deutsche Bank, despite public statements that it was cooperating fully with authorities, found itself the target of the largest dawn raid in German history on December 12, 2012, with more than 500 prosecutors and police officers searching employees' offices and homes in Frankfurt, Berlin and Dusseldorf. Prosecutors said they were investigating 25 bank staff on suspicion of severe tax evasion, money laundering and obstruction of justice. Der Spiegel, "Head Office Raided in Tax Probe: Deutsche Bank CEO Under Investigation", December 12, 2012, http://www.spiegel.de/international/business/deutsche-bank-co-ceo-juergen-fitschen-under-investigation-in-tax-probe-a-872563.html Prosecutors claimed that Deutsche Bank did not adequately respond to authorities' prior information requests. Gibson Dunn 2012 Year-End German Law Update "Compliance - Public Investigations on the Rise" at 22, http://www.gibsondunn.com/publications/pages/2012YearEnd-GermanLaw-Update.aspx

46 Gesetz zur Regelung der Verständigung im Strafverfahren, BGBl. I.S. 2353; see also ICID Review, Spring 2010 "Cooperation with German Investigation Authorities" at 1, 10-12.

About Patrick J. Burke

Patrick J. Burke serves as Counsel in the New York office of Reed Smith LLP (pburke@reedsmith.com, tel: 212.549.0313), where he works with the firm's Records and E-Discovery Group and counsels clients in the areas of electronic discovery, privacy, records management, information governance, and cybersecurity. He holds the Certified Information Privacy Professional certification for European data privacy (CIPP/E). Patrick is an Adjunct Professor at the Benjamin N. Cardozo School of Law, where he teaches "E-Discovery, Digital Evidence and Computer Forensics."

Patrick gratefully acknowledges the valuable contributions by his Legal Intern at Reed Smith, Donna Salcedo.

Our Customers

Guidance Software customers are corporations and government agencies in a wide variety of industries, such as financial and insurance services, technology, defense contracting, pharmaceutical, manufacturing and retail. Representative customers include Allstate, Chevron, FBI, Ford, General Electric, Honeywell, NATO, Northrop Grumman, Pfizer, SEC, UnitedHealth Group, and Viacom.

About Guidance Software (NASDAQ: GUID)

Guidance Software is recognized worldwide as the industry leader in digital investigative solutions. Its EnCase® Enterprise platform is used by numerous government agencies, more than 65 percent of the *Fortune 100*, and more than 40 percent of the *Fortune 500*, to conduct digital investigations of servers, laptops, desktops, and mobile devices. Built on the EnCase Enterprise platform are market-leading electronic discovery and cyber security solutions, EnCase® eDiscovery and EnCase® Cybersecurity, which enable organizations to respond to litigation discovery requests, proactively perform data discovery for compliance purposes, and conduct speedy and thorough security incident response. For more information about Guidance Software, visit www.encase.com.

For more information about Guidance Software, visit www.encase.com.