

Obtaining German Works Council Approval to Collect Employee E-mail and Electronic Documents

Patrick J. Burke, Esq.

I. Executive Summary

Companies that seek to collect German employee E-mails and electronic documents all confront the same hurdle: obtaining permission from their company's works council. Germany's works councils have earned a reputation as fierce protectors of employee privacy rights, often rejecting corporate efforts to search through employee data. Their opposition invokes the rights and protections afforded German employees pursuant to the 1995 E.U. Data Protection Directive as well as German federal and state data protection laws.

This white paper will address several questions that arise in dealing with German works councils, such as

- What is a works council and how do they function?
- What is the German data protection regime upon which the works councils can base their objections?
- What steps can a company take to maximise the probability that its data collection methodology will be approved by its works council?

The suggested approaches to the works councils are based on interviews with two Guidance Software customers who successfully obtained works council approval at their companies for automated collection of employee E-mail and electronic documents using EnCase® Enterprise and Guidance's own experience. Each of these major non-German corporations – one an auto maker and the other a manufacturer of computer components – showcased the functionality of EnCase Enterprise as an essential part of their successful applications.

II. The Works Council

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.¹

Works councils are established through democratic processes. Candidates for works councils must secure a certain amount of signatures from their fellow employees to be eligible for election.² Trade unions may also nominate candidates for election, but cannot compel their members to vote a specific way.³ Works council members are elected directly by company employees through a secret ballot, though employees are not required to vote,⁴ and generally serve for four years.⁵ The size of a works council depends on the number of employees within a company and the Works Constitution Act also requires works councils to proportionately represent certain types of employees.⁶

Under the Works Constitution Act, works councils have the right to co-determination in matters affecting company structure, personnel decisions, and policies regulating workplace and individual conduct within the company.⁷ The rights of a works council can be categorised as follows:

- **Information:** The works council has 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 works council has the right to consult and cooperate with management to jointly discuss and develop the topic at issue.
- **Veto Right:** A works council has the right to block certain management decisions.

The employer is required to keep the works council fully informed in matters relating to operations and personnel planning so that the council can participate in drafting company policy.⁸ The purpose of this is to allow the works council to cooperate with management to avoid potential disputes and raise relevant concerns or other suggestions.

The works council resolutions require a quorum of fifty percent and resolutions are adopted by simple majority unless otherwise required by law.⁹ Works councils and management may, formally or informally, enter into valid and binding agreements;¹⁰ formal agreements are immediately binding on employer 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 on it. 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 work force.¹¹

In the event that disputes between works councils and management cannot be resolved amicably, the parties may be assisted by the conciliation board, a body with arbitration and mediation duties.¹² Assuming that 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.¹³

III. German Data Protection

When works councils assert their right to approve or disapprove employee data collection methodologies, they are in part invoking their rights pursuant to European Union law, German federal law, and the data protection laws of their home states. The EU Data Protection Directive authorises the processing of employee data as long as it is necessary to protect the legitimate interest of another party and as long as the employee's interests and fundamental freedoms are not overridden.¹⁴ Each member state has enacted legislation that effectuates the general tenets of the EU Directive.

Germany's Federal Data Protection Act (*Bundesdatenschutzgesetz*) regulates the collection of personal data as well as the storage, alteration, transfer, blocking, deletion and use of such data.¹⁵ It also allows for collection of employee data under certain circumstances and calls for a balance between the legitimate business purposes of the company and the legitimate privacy interests of affected employees.¹⁶ In some situations, employee notification and even consent are required for collection of personal data.¹⁷ The Federal Data Protection Act regulates compliance with the law through company self-monitoring and external government oversight. It also differentiates between criminal and administrative violations of the law as well penalties for such infractions.

Data protection is also regulated on the state level. The German states all maintain data protection laws that mirror the Federal Data Protection Act.¹⁸ 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.¹⁹ The State Commissioner also oversees private organisations within its jurisdiction to ensure compliance with the state data protection law.²⁰ Like

the Federal Act, the state data protection laws provide for notification and the obtaining of consent before processing of personal data can take place.

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 and are empowered to investigate violations. These commissioners may also perform audits to ensure that a company's organisational and technological safeguards sufficiently comply with the applicable data protection law.²¹

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 BDSG at the state and federal levels.²² 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.²³

IV. Securing Works Council Approval to Collect Employee Data

Works councils are different in every company, and each company has an individual relationship with their works councils that will affect their presentation on this topic. We interviewed two major companies with substantial facilities in Germany (although based outside of Germany) that have recently received permission from their works councils for collection of employee e-mail and electronic documents. The two companies – one automotive and the other a manufacturer of computer components – use the EnCase Enterprise technology for collection and both emphasised its use in their applications to their works councils.

Based on the experience of those two companies, as well as suggestions from other major companies with operations in Germany, we offer the following suggestions for successful works council applications:

- **Get on the works council agenda as early as possible.** Usually this is handled through the company's HR department, which generally interfaces with the works council. In the case of the auto maker, it took 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, they should also attend, both out of respect and to be available for tough questions.
- **Emphasise that EnCase Enterprise can enable you to avoid collecting employee personal E-mail or documents.** With EnCase Enterprise, 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 collections will be done “in-country”.** Some works councils are reassured when told that all collections will be done from within Germany, rather than operated from a location in another European member state or else outside Europe. EnCase Enterprise

- technology allows for an “examiner” (a laptop or workstation from which the EnCase search is operated) to be placed inside Germany, even if that is not its usual location.
- **Discuss how EnCase Enterprise can be configured to prevent employee data from being transferred outside Europe.** EU data protection laws permit transfers to other European jurisdictions, but prevent most transfers outside Europe. EnCase Enterprise can be configured to prevent searches of European employee data from outside of Europe, and prevents the transfer of data collected to locations outside Europe.
 - **Emphasise that existing investigative policies already approved by the works council will remain in place.** For example, HR policies relating to the investigation of potential employee wrongdoing had long ago been approved by the works council and will not be affected by the use of EnCase Enterprise technology. That data would go directly to the company’s HR team and would be handled the same as before.
 - **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, EnCase Enterprise’s search criteria can be configured to leave that folder untouched, so that none of that data will be 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 Enterprise, these file types can be excluded.

V. Conclusion

Companies seeking approval from works councils, particularly companies based outside of Germany, must approach their works councils with sensitivity toward the interest in the protection of the employee’s personal data. This sensitivity is often not enough to obtain the works council’s blessing for a collection methodology; the concerns are that the collection methodology may expose personal employee information and the employee data may be accessed from outside Germany. To gain approval, the collection methodology itself must reflect proactive strategies – including procedures and technology – to guarantee that employees need not be concerned that their private e-mail and electronic documents will be collected along with those the company requires for legal purposes.

As the automotive and computer component companies learned, the use of EnCase Enterprise technology can serve as an invaluable part of that guarantee of compliance with data protection laws.

APPENDIX I: Key Players

Federal Data Protection Commissioner:

Data Protection Commissioner who is elected by the German Parliament for a term of six years and is independent in the exercise of his duties and 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 that provide 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 organisations. These officers are responsible for (1) controlling data by preventing unauthorised 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 authorisation; (4) 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 organisational 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://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML>

German Federal Data Protection Act (in English):

http://www.bfdi.bund.de/cln_007/mn_946430/EN/DataProtectionActs/Artikel/Bundesdatenschutzgesetz-FederalDataProtectionAct.templateId=raw.property=publicationFile.pdf/Bundesdatenschutzgesetz-FederalDataProtectionAct.pdf

Works Constitution Act (in English):

<http://hikwww1.fzk.de/br/content/worksConstitutionAct-BetrVG.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 (in English):

http://www.lda.brandenburg.de/sixcms/media.php/2232/bbgdsg_e.pdf

Hamburg:

<http://fhh.hamburg.de/stadt/Aktuell/weitere-einrichtungen/datenschutzbeauftragter/datenschutzrecht/hamburgisches-datenschutzgesetz-1990-07-05-pdf.property=source.pdf>

Hesse:

<http://www.datenschutz.hessen.de/hdsg99.htm>

Mecklenburg-Vorpommern:

http://www.lfd.m-v.de/dschutz/ges_ver/guv/guv_c_20.html

Lower Saxony:

http://cdl.niedersachsen.de/blob/images/C2643488_L20.pdf

North Rhine-Westphalia:

<https://www.ldi.nrw.de/>

Rhineland-Palatinate:

http://www.datenschutz.rlp.de/rgrundlagen/a1_5.html

Saarland:

http://www.lfdi.saarland.de/html/lfd-internet/datenschutzrecht/sdsg_2007.pdf

Saxony:

<http://www.sachsen.de/de/bf/staatsregierung/ministerien/smi/smi/upload/SachsDSG2003.pdf>

Schleswig-Holstein (in English):

<https://www.datenschutzzentrum.de/material/recht/lhsg-eng.htm>

Thuringia:

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

NOTES

- ¹ See Works Constitution Act (Betriebsverfassungsgesetz) §1, available at <http://hikwww1.fzk.de/br/content/worksConstitutionAct-BetrVG.pdf>
- ² Works Constitution Act §14(2).
- ³ Works Constitution Act §14(5).
- ⁴ Works Constitution Act §14(1).
- ⁵ Works Constitution Act §21.
- ⁶ Works Constitution Act §15(2).
- ⁷ Ingebjörg Darsow, *Implemenation of Ethics Codes in Germany: The Wal-Mart Case*, Universität Pompeu Fabra, (March 2005) available at <http://www.upf.edu/iuslabor/032005/art11.htm>.
- ⁸ Works Constitution Act §80, 81, 85, 89.
- ⁹ Works Constitution Act §33.
- ¹⁰ Works Constitution Act §77.
- ¹¹ Works Constitution Act §77(5).
- ¹² Works Constitution Act §76.
- ¹³ Works Constitution Act §96.
- ¹⁴ Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995, Section II, art. 7, 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>
- ¹⁵ Federal Data Protection Act (Bundesdatenschutzgesetz,) §1, available at http://www.bfdi.bund.de/cln_007/nn_946430/EN/DataProtectionActs/Artikel/Bundesdatenschutzgesetz-FederalDataProtectionAct,templateId=raw,property=publicationFile.pdf/Bundesdatenschutzgesetz-FederalDataProtectionAct.pdf.
- ¹⁶ Federal Data Protection Act §10(1).
- ¹⁷ Although the Federal Data Protection Act specifies several times that notification of the data subject is required, Section 33 of the Federal Act provides exceptions to the requirement of notification and consent, including:
- if a data subject has otherwise received notification such that it is unnecessary to inform the subject a second time;
 - if there is an overriding interest that requires the storage of the data in secrecy due to a legal interest of a third party;

-if the data will be erased within three months;
-if it is for a business's own purposes and can either be found from generally accessible sources or notification would "considerably impair the business purposes of the controller."
Federal Data Protection Act § 33(6)(b).

¹⁸ See Sidebar titled "Useful Links" for links to various state data protection laws.

¹⁹ See, e.g., Bavarian Constitution, Art. 33(a), available at http://www.bayern.landtag.de/en/bayer_verfassung_erster_hauptteil.html#4; Saxony-Anhalt Data Protection Act, §20, available at http://www.sachsen-anhalt.de/LPSA/fileadmin/Elementbibliothek/Bibliothek_Politik_und_Verwaltung/Bibliothek_LF/D/PDF/binary/Vorschriften/Land/dsg-Isa/English/par19_ut_to_24.pdf

¹⁹ Saxony-Anhalt Data Protection Act, §22.

²⁰ Saxony-Anhalt Data Protection Act, §22.

²¹ Federal Data Protection Act §38.

²² Federal Data Protection Act §4(f).

²³ Federal Data Protection Act §4(f)(5).

ABOUT PATRICK J. BURKE

Patrick J. Burke, Assistant General Counsel at Guidance Software, Inc., previously practiced in the commercial litigation department of Linklaters, where he served on the firm's eDiscovery Working Group. Patrick gratefully acknowledges the valuable contributions by his Legal Interns Lawrence Estrada and Krystal Juncosa.

ABOUT GUIDANCE SOFTWARE (GUID)

Guidance Software is recognised worldwide as the industry leader in digital investigative solutions. Its EnCase[®] platform provides the foundation for government, corporate and law enforcement organisations to conduct thorough, network-enabled, and court-validated computer investigations of any kind, such as responding to eDiscovery requests, conducting internal investigations, responding to regulatory inquiries or performing data and compliance auditing – all while maintaining the integrity of the data.

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

This paper is provided as an informational resource only. The information contained in this document should not be considered or relied upon legal counsel or advice.

