the Constitution of Enterprises (BVG). This right is also guaranteed by the data protection law when data is administered by a third party.

The data processing firm is an authorized party. The court ruled that EDS could not be considered an unauthorized third party whose access to data is prohibited by Article 2, Paragraph 2, of the data law because EDS's right to the data is given through its mandate from Opel to process the data.

Illegal data exports are a risk but not a danger. Setting up an EDS subsidiary in Germany to handle Opel's data turned out to be a legally sound move (both are located in Russelsheim, near Frankfurt). The court rejected IG Metall's claim that Article 24 on transborder data transfer was violated. There was a "theoretical possibility" that individual items of data could be sent outside Germany, the court said. But supervising such incidents is part of the general question of supervising data storage, and the "theoretical possibility" is not an indication of a "concrete danger" that EDS would send Opel data illegally out of the country.

The data processing firm is qualified for the task. Opel's claim about EDS's qualifications was not contested by the union, the court noted, and it ruled that there were no grounds for maintaining that the auto firm had not exercised appropriate care in selecting an outside data processing firm (Article 8). For the same reason, the court added, there were no grounds for claiming that Opel had neglected its workers' interests in letting EDS store and process company data.

Violation of constitutional rights did not occur. IG Metall's contention that turning the data over to EDS had violated Opel workers' constitutional right to information also got nowhere. That could not apply to a legally made contract, the court decided.

IG Metall has announced that it will appeal against the court's decision.

DATA PROTECTION MANAGEMENT CHECKLIST

Data protection laws give rights to individuals on whom data records are kept to gain access to those records and correct them if they are wrong. Companies should now make sure that they are prepared for the tensions that could develop when employees read managers' evaluations of their performances.

To help minimize potential problems, companies should appoint a manager who is responsible for complying with data protection legislation. He should ensure that he knows:

+ where the company's name-linked files are kept;

+ who manages them and is responsible for training staff on data security procedures;

+ whether there is a companywide policy on how frequently to review records to ensure they are up to date;

+ whether there is an agreed maximum period before records are destroyed;

+ whether name-linked files are registered with the appropriate authorities in each country where this is necessary;

+ whether the company's export of data complies with national law and has the appropriate national approval;

+ whether by complying with US law on monitoring the employment of minority ethnic groups the company data files will conflict with any European national laws on compiling sensitive data on racial or ethnic groups.

PRIVACY LAWS AND FINANCIAL INFORMATION

The introduction of data protection legislation will affect two main areas of financial information:

+ data on individuals' bank accounts, insurance policies etc.,

+ data on individuals' credit worthiness.

In the first case, the individual knows that he has a bank account or an insurance policy and which financial institution he deals with. He has a contractural relationship and if he wishes to seek access to his record to exercise his data protection rights, he knows where he must make his request.

The second case is quite different in data protection terms because in this instance the individual data subject does not normally have a contractural relationship with the data owner. The credit information company can collect information on an individual and supply it to a third party without the data subject being aware of the process. The data subject may be aware of the data collection process only when he seeks and is refused credit or is granted credit at unfavorable terms.

For this reason credit information has been regulated by separate laws in some countries, for example, Sweden and the UK. Indeed in the UK, the Consumer Credit Act of 1974, giving individuals a right of access to their credit information records, was passed a