SQUIRE PATTON BOGGS

ANTI-TERRORIST SCREENING OBLIGATIONS
Employers on the Horns of a Dilemma

As a result of the terrorist attacks on 11 September 2001, the European Union has also increased its counter-terrorism efforts. The goal is thereby to block the economic activities of terrorists amongst other things. Private sector companies should also provide support in this regard by preventing cash flows to persons or organizations named on anti-terrorism lists. The so-called prohibition of aid principle has been laid down in the EU anti-terrorism regulations. According to this principle, it may be prohibited to hire, employ or pay wages to suspected terrorists. This obligation not only exists for banks and financial service providers but also in principle for all EU-related companies and above all for any such companies involved in foreign trade. According to surveys, many companies are unaware of this fact or simply fail to comply with the existing obligations.

One reason for this lack of compliance may be the existing legal uncertainties in the area of tension between monitoring obligations and data protection. Ultimately, companies will not be able to avoid carrying out so-called anti-terrorist screenings, i.e., comparing the data of their employees with the EU anti-terrorism lists. Otherwise, they could be subject to criminal liability under foreign trade law or face commercial sanctions. One incentive for conducting anti-terrorist screenings is therefore, for example, the possibility of being recognized as an "Authorized Economic Operator" (AEO).

Data Protection Concerns

Companies are faced with a dilemma when clarifying whether anti-terrorist screenings are legally permissible: If they don't "screen," they may possibly be violating EU law or national anti-terrorism legislation; if they do "screen," they are potentially violating data protection law. Both are subject to sanctions, whereby the legal situation is extremely controversial and a uniform implementation practice does not exist. Neither reliable, generally accepted court decisions are available nor does draft legislation on employee data protection provide any further assistance.

Whether general anti-terrorist screenings are even permitted in Germany under data protection law depends on the controversial issue whether the EU anti-terrorism regulations provide the required legitimacy in this regard.

It is widely held that the consent of the data subject cannot form the legal basis for such screenings. While the German Federal Government and Fiscal Court base the anti-terrorist screenings on the EU anti-terrorism regulations, the "Düsseldorfer Kreis" – an association consisting of the federal and state data protection officers – does not consider this to be a sufficient legal basis.

In practice, anti-terrorist screenings are partially conducted in reference to Section 28 German Federal Data Protection Act, which requires, however, weighing the interests of the employer and the employee amongst other things. Depending on the constellation of the individual case, the ECJ has already decided that the interests of the employee could eventually prevent such screenings if necessary.

Works Agreements

Works agreements can create more reliability; however, the regulations of such agreements must be carefully prepared because the anti-terrorism regulations of the EU do not stipulate how anti-terrorist screenings are to be conducted. It should especially be clarified with the works council which employee data can be the object of such screenings, whether, for example, addresses or certain information found on identity cards are also included, and how cases of suspicion are to be handled.

How Are Screenings To Be Conducted?

An obligation to conduct screenings manually should be considered unreasonable for the employer at most companies due to the high number of employees. On the other hand, automated screenings involve methods, which are associated with the greatest infringements of personal rights of employees. The possibility of data anonymization during the initial step or pseudonymization should be taken into consideration.

Due to the fact that documentation obligations are also assumed to exist with respect to anti-terrorist screenings, companies should also always document the reason, scope and circumstances surrounding the screenings or reach an agreement with the works council in this regard respectively.

Commissioning an external service provider to conduct the screenings can be an option but is only permissible to a limited extent and must be covered by special (data protection) contracts.

Last but not least, the question is which employees must be screened. As a rule of thumb: The more relevance the work of an employee has for security issues, the more likely such screening will be required or permitted. However, whether and how the screening is conducted always requires taking the overall circumstances at the company or group of companies as well as the area of economic activities into sufficient consideration.

Contact

Dr. Annette Demmel
Partner
Certified Specialist for Information Technology Law

Squire Patton Boggs (US) LLP
Unter den Linden 14
10117 Berlin

E annette.demmel@squirepb.com
T +49 30 726 16 8226