

EU

Court of Justice of the European Union: No “Right to be Forgotten” for Personal Data in a Register of Companies

The Court of Justice of the European Union (CJEU) [ruled on 9 March 2017](#) that natural persons participating in trade must accept the disclosure of a limited amount of their personal data (relating to their identity and functions within the company) in a register of companies even upon dissolution of the company. The CJEU explained that the reasons for this ruling were rooted in the need to protect the interests of third parties and to ensure legal certainty. Only in exceptional instances, on the basis of a case-by-case assessment, could there be legitimate reasons for member states to restrict access to such personal data after the expiry of a sufficiently long period after the dissolution of the company.

The background to the ruling was a preliminary reference by the Italian *Corte Suprema di Cassazione*, which wanted to know whether the EU Data Protection Directive (95/46/EC) and Directive 68/151/EEC prohibited timely, unlimited access of natural persons to personal data in a register of companies.

France

Decision on Outdoor Wireless Audience Measuring Tool

In a decision handed down on 8 February 2017, the [Conseil d’Etat ruled in favour of the French data protection authority](#), the CNIL, after it refused to authorise a well-known advertising company to test a new audience measuring tool on the flow of pedestrians in a specific location. The company in question proposed to use WiFi counting boxes placed on billboards to capture the MAC addresses of mobile devices within a range of 25 metres. The purpose of the tool is to count the number of people passing by the billboards, to identify their direction of movement and count the number of repeat visits.

The Conseil d’Etat held that there was insufficient information for data subjects, noting that a proposed information notice would not have been prominent enough to cover the entire range of the tracking device. In addition, the Conseil d’Etat found that the advertising company had not considered data subjects’ rights to object, to access their data and to ask for rectification (however, it was considered that the consent of the data subjects was not required).

The Conseil d’Etat also considered the proposed methods for the anonymisation of data to be problematic. The advertising company argued that it planned to “anonymise” the data by truncating and blurring MAC addresses (according to the “salting” and “hash key” methods).

Thus, according to the company, the risk of identification was negligible. However, it was considered that it was still possible for the administrator to re-identify the data subjects. The anonymisation envisaged was, therefore, incomplete. Moreover, the purpose of the processing, to identify the movements of persons and the number of repeat visits throughout the duration of the test, was considered to be incompatible per se with the anonymisation of the data.

CNIL Publishes Model for Processing Activities

The CNIL (French data protection authority) has [published a model](#) for the records which data controllers and processors are required to keep under the General Data Protection Regulation (GDPR). Data controllers and processors will need to maintain a record of their data processing activities when the GDPR comes into force in May 2018, and the CNIL’s model provides a form that controllers and processors can use for this purpose.

Germany

Data Protection Authorities: Amendment of the Law on the Federal Criminal Police Office Interferes With Privacy

The Conference of the Independent Data Protection Authorities of the *Bund* and the *Länder* has [issued a resolution](#) stating that the government draft of the amendment of the law on the Federal Criminal Police Office (*Bundeskriminalamtsgesetz*) needs to be revised due to infringements of fundamental rights, including privacy. According to the Conference, the stipulated restrictions of privacy, such as extensive data storage or loosened procedural safeguards, are not required either by the decision of the German Constitutional Court on the *Bundeskriminalamtsgesetz* from April 2016 or by EU Directive 2016/680 on data protection in the area of justice and home affairs.

UK

ICO Issues GDPR Guidance to Local Authorities

The Information Commissioner’s Office (ICO) has reported on the results of a [survey of local](#) authorities on their preparedness for the General Data Protection Regulation (GDPR) that it conducted last year. The standout findings of the survey were that a quarter of councils do not have a data protection officer, 15% of councils do not have data protection training for employees involved in processing personal data and a third of councils do not undertake privacy impact assessments. The ICO reminded councils that under the GDPR, they will be obliged to appoint a data protection officer and to undertake privacy impact assessments in certain circumstances. Local authorities were also reminded of their responsibility to ensure that all staff involved in processing personal data, including temporary staff, receive adequate training.

Contacts



Philip Zender
Partner, San Francisco
T +1 415 393 9827
E philip.zender@squirepb.com



Francesca Fellowes
Senior Associate, Leeds
T +44 113 284 7459
E francesca.fellowes@squirepb.com



Stephanie Faber
Of Counsel, Paris
T +33 1 5383 7400
E stephanie.faber@squirepb.com



Annette Demmel
Partner, Berlin
T +49 30 7261 68 108
E annette.demmel@squirepb.com



Caroline Egan
Consultant, Birmingham
T +44 121 222 3386
E caroline.egan@squirepb.com



Emma Garner
Associate, Leeds
T +44 113 284 7416
E emma.garner@squirepb.com

The contents of this update are not intended to serve as legal advice related to individual situations or as legal opinions concerning such situations nor should they be considered a substitute for taking legal advice.