

UK

ICO Publishes Big Data Report

The Information Commissioner's Office (ICO) has published its Big Data report. The report explains which aspects of data protection law organisations need to particularly consider when undertaking big data analytics and suggests steps they can take to achieve compliance.

[ICO – Big Data and Data Protection, 28 July 2014](#)

ICO Review of Civil Monetary Penalties

The ICO has published its review of the impact of civil monetary penalties (CMPs), assessing the extent to which CMPs improve data protection compliance. The report concludes that CMPs are effective at improving data protection compliance, particularly by organisations issued with a CMP but also amongst peer organisations, where CMPs had a wider impact as a deterrent and incentive to "get it right first time".

[ICO – Review of the impact of ICO civil monetary penalties, 28 July 2014](#)

ICO Serves £50,000 Monetary Penalty for Nuisance Calls

The ICO has imposed a monetary penalty of £50,000 on a digital marketing company for breaches of the Privacy and Electronic Communications Regulations. The company had made unsolicited marketing calls to people who had registered with the Telephone Preference Service (TPS), resulting in 481 complaints to the TPS and 120 complaints to the ICO over a one year period.

[ICO News Release – Digital Marketing Company receives £50,000 penalty for bombarding people with nuisance calls, 28 July 2014](#)

House Of Lords Committee Criticises Right to Be Forgotten Ruling

The House of Lords EU Home Affairs, Health and Education Sub-Committee has said that the Court of Justice of the European Union's recent "right to be forgotten" ruling is "misguided in principle and unworkable in practice". After hearing evidence, the Chairman of the Sub-Committee said that the ruling was unworkable because of the significant resources required by search engines to process removal requests and because search engines should not be required to sit in judgement on whether to remove data or not based on "vague, ambiguous and unhelpful criteria". She said that individuals should not be able to have information about them removed simply because they do not like what is said. The UK government must continue to fight, she said, to ensure that the new Data Protection Regulation does not class search engines as data controllers or contain a right to be forgotten or right to erasure provision, which would effectively give individuals rights which were unenforceable.

[parliament.co.uk – Lord Select Committee, 30 July 2014](#)

Compliance With the Principles of Reciprocity on Data Sharing

The Steering Committee on Reciprocity (SCOR), the body established by the UK finance industry, has announced that all firms that share consumer and commercial credit performance data through credit reference agencies must undergo a compliance exercise to confirm that the data sharing complies with the Principles of Reciprocity (the latest version of which was approved in June). The exercise will begin in September 2014 and will require the completion of an online questionnaire. Separately, following talks between SCOR and the Financial Conduct Authority (FCA), the FCA has stipulated that shared data must be accurate, to facilitate responsible lending assessments, and that firms must take reasonable steps to maintain accurate and adequate data, to ensure that the correct customer is pursued for the correct amount of debt.

[Scoronline.co.uk – Principles of Reciprocity](#)

Germany

German Federal Supreme Court Confirms Seven Day Retention Period for Dynamic IP Addresses

The German Federal Supreme Court recently handed down a ruling confirming that Internet Service Providers (ISPs) are allowed to retain the dynamic IP addresses of their customers for a period of seven days, under the German Telecommunications Act. The court considered that the collection and use of this data was suitable, necessary and appropriate for countering any threats to the functionality of the ISP's telecommunications operations. It considered that, in light of the current state of technology, there were no other options available to ISPs for identifying, isolating and, if necessary, remedying any disruptions to the telecommunications system. The court said that the ECJ's recent invalidation of the Data Retention Directive did not affect this position.

[Judgment of the German Federal Supreme Court \(Bundesgerichtshof\), July 2014 \(German language\)](#)

France

CNIL Imposes Fine for Unlawful GPS Tracking System

Following an investigation, the CNIL has imposed a fine for data protection breaches on a luxury car rental company. The fine of €5,000 was imposed for use of an unlawful GPS tracking system on rented cars. The CNIL found the fine justified because, amongst other things, the tracking system had not been registered with the CNIL, customers were unaware of its use, it was disproportionate as collecting data on a 24/7 basis rather than merely in the event of theft or failure to return the car and access to the data had not been adequately secured (the password had not been changed for two years). The CNIL does not automatically publish details of all of the fines it imposes. Public notice of a fine is used by the CNIL as an additional sanction.

[CNIL - notice of fine, 28 July 2014 \(French language\)](#)

Second CNIL Fine for Data Protection Breaches

The CNIL has imposed a fine of €3,000 on the Fédération Française d’Athlétisme for data breaches around the publication of sports results. The CNIL found that the Fédération had failed to give non-licensed athletes proper notice that their individual results, achieved in their particular sports event, would be published on the official Fédération Française d’Athlétisme website, even though to do so would not have required disproportionate effort. The CNIL also found that the Fédération had failed to implement sufficiently robust security measures to ensure that the personal data it processed remained confidential.

[CNIL – notice of fine, 28 July 2014 \(French language\)](#)

New Norms for the French Public Sector

The CNIL has published a compliance package for providers of social housing comprising three standardised norms for the processing of personal data. The first relates to the evaluation of social difficulties (autorisation unique AU-35) and the second concerns the management of litigation and enforcement of court orders (autorisation unique AU-034). The CNIL has also created a norm concerning the exchange of data between cities for the purpose of crime prevention (autorisation unique AU-038).

[CNIL article, 22 July 2014 \(French language\)](#)

EU

WP29 Meets With Search Engines to Discuss Right to Be Forgotten

The Article 29 Working Party (WP29) met with representatives of the major search engines to discuss the practical implementation of the CJEU’s recent “right to be forgotten” ruling and to provide input on new WP29 guidance. The guidance will assist national data protection authorities in handling complaints from individuals whose erasure requests had been refused. At the meeting, the search engines were asked to explain the logistics of a delisting request, including what information they require in a request, whether requests are filtered on the basis of location, nationality, or place of residence of the individual, on which domains delisting takes place (EU or global), what criteria is used to balance the right of erasure against the right of the public to have access to the information, what grounds are used to justify a refusal to delist and whether website publishers are notified of the delisting. The search engines have been asked to answer a number of additional questions in writing by 31 July. WP29 may arrange future meetings and its guidance is expected in the Autumn.

[WP29 Press Release, 25 July 2014](#)

New Regulation on Electronic Identification

The European Council has adopted a new Regulation which lays down conditions for the mutual recognition of electronic identification across EU member states and sets rules for trust services. The Regulation provides for member states to individually adopt national electronic identification schemes (such as a framework for electronic signatures) which must then be recognised by all other member states once notified to the EU Commission. The Regulation also introduces EU wide rules concerning trust services, such as the creation and validation of certificates for website authentication, and a related EU trust mark for those services which meet the requirements of the Regulation. The Regulation will apply from 1 July 2016.

[Council of the European Union Press Release, July 2014](#) and [Regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market](#)

New Standards for Data Protection Compliance by Users of RFID

New EU technical standards have been agreed that will help users of Radio Frequency Identification (RFID) smart chips and systems to comply with data protection requirements. The standards require organisations using smart chips to give consumers information on what personal data will be collected via the chips and why, promote consumer awareness that smart chips are being used by the use of a common European symbol and to carry out private impact assessments, for review by national data protection authorities, before using smart chips. The standards provide that consumer surveillance must not be undertaken using RFID chips, but these chips should be deactivated by default immediately and free of charge at the point of purchase.

[European Commission Press Release, 30 July 2014](#)

Data Regulation Could Slow Pace of Cancer Research

The European Society of Medical Oncologists (ESMO) has issued a position paper warning that the consent requirements in the new draft General Data Protection Regulation could jeopardise progress on cancer research. The ESMO has said that the Regulation as drafted appears to require patients to give specific consent to each new use of their data and tissue for research. It says that the Regulation should be amended to allow researchers to obtain one-off “forever” consent from patients to all research, subject to the right to withdraw the consent at any time.

[Risks of the new EU Data Protection Regulation: an ESMO position paper endorsed by the European Oncology Community, July 2014](#)

Russia

Changes to Russian Data Protection Law

Vladimir Putin, President of the Russian Federation, has signed changes to Data Protection Law. The law, which will take effect on 1 September 2016, will prohibit the storage of personal data of individuals collected in Russia, including via the Internet, in data centers located outside Russia. This restriction does not apply if storing personal data in foreign data centers is:

- expressly allowed under international treaty or other federal law;
- necessary for the administration of justice or enforcement proceedings (administration of justice by the Russian state courts only; processing personal data necessary for the administration of justice by a foreign court and for foreign enforcement proceedings generally will not be allowed unless a writ of execution is issued by a Russian state court; arbitration proceedings are not deemed as the administration of justice);
- necessary for the provision of public/municipal services by Russian state and municipal authorities; and
- necessary to implement the journalist's professional activity and (or) the legitimate activities of the mass media or the scientific, literary and creative activities.

[Amendment to Part IV of the Civil Code of the Russian Federation](#)

Squire Patton Boggs' Second Pan-European Employment Event – Now Expanded To Include EMEA Countries

On 1-2 October, our London office will host our second Pan-European Employment event of 2014. Lawyers from 15 countries across the EMEA will be available to meet with delegates, in one to one meetings of up to 30 minutes each, to discuss any of the following topics:

- Labor & Employment Law
- Taxation and International Benefits
- Data Privacy
- Pensions

For more details, and to reserve a place, please [click here](#).

For further information on any of the items in this week's alert, please contact:

Mark Gleeson

T +44 20 7655 1465

E mark.gleeson@squirepb.com

Annette Demmel

T +49 30 72616 8226

E annette.demmel@squirepb.com

Stéphanie Faber

T +33 1 5383 7400

E stephanie.faber@squirepb.com

Irina P. Golovanova

T +7 495 258 5250

E irina.golovanova@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.

© Squire Patton Boggs.