

UK

Ministry of Justice Fined £180,000 for Security Breaches

The Information Commissioner's Office (ICO) has fined the Ministry of Justice (MOJ) £180,000 for repeated serious failings in the secure handling of personal data by the prison service. In October 2011, an unencrypted hard drive containing sensitive prisoner data was lost. The MOJ issued new encryption capable hard drives, but the prison service was unaware that the encryption option needed to be turned on for it to work. Subsequently, a second hard drive was lost, which should have been encrypted but was not. As a result, the ICO found that the prison service was handling highly sensitive data insecurely and imposed the fine.

[ICO news release – 26 August 2014](#)

ICO Publishes Local Authority DPA Compliance Report

The ICO has published the findings of the audit it carried out last year into local authority compliance with the DPA. The report concludes there is "clear room for improvement", particularly in staff training and effective data protection governance. The report also highlights examples of best practice found during the audits, including in records management and data security procedures.

[ICO news release – 26 August 2014](#)

ICO Raises Awareness of the Privacy Implications of the Internet of Things

In a blog post, the ICO has warned about the data protection implications of 'The Internet of Things' (network connected objects, such as household devices, often able to be operated remotely via an internet connection). The ICO explains how much of the information being processed during the interaction with these devices will amount to personal data and discusses the potential security concerns. It highlights the need for manufacturers of these smart devices to ensure they are DPA compliant and urges the public to educate themselves on the potential privacy risks.

[ICO blog post – 21 August 2014](#)

Government Consults on Reuse of Public Sector Data

The Government is consulting on the implementation in the UK of Directive 2013/37/EU on the reuse of data produced and collected by public bodies. The Directive aims to harmonise the rules across the EU around the reuse of public sector information, encouraging an open data approach but with the option for public bodies to charge for reuse. The consultation invites comments on how, in the UK, these charges should be calculated and on the appropriate appeals procedures against adverse public sector decisions on reuse. The consultation closes on 7 October 2014.

[Gov.uk – Open consultation on UK implementation of Directive 2013/37/EU on the reuse of public sector information – August 2014](#)

ICO Warning to Businesses on the Threat of Online Attacks

The ICO has warned businesses that they must have adequate IT security procedures in place to withstand a targeted online attack. The warning came as the ICO issued a news release confirming that the Racing Post had signed an undertaking committing to improve its IT practices after its website was hacked and the personal data of 677,335 of its customers compromised. An ICO investigation found that the Racing Post had failed to apply up-to-date security patches leaving the website vulnerable to attack.

[ICO news release – 28 August 2014](#)

EU

France

CNIL Warns Against Use of Licence Plate Recognition Devices

The French Data Protection Authority, the CNIL, has warned French counties and municipalities that they are not permitted to implement devices allowing automated licence plate recognition of vehicles in the region. These devices raise privacy concerns as they are linked to the use of CCTV, which reads and records the licence plates (and occupants) of all vehicles entering or leaving the region over an indeterminate period. The CNIL confirms that, in the absence of a specific regulatory act covering counties and municipalities, only the national police, gendarmerie and customs authorities are empowered by law to use licence plate recognition devices to prevent serious crime and protect public order.

[CNIL article – August 2014](#)

CNIL Warns Orange over Security and Confidentiality Breaches

The CNIL has issued a public warning to the telecommunications provider Orange over security and confidentiality breaches. In April 2014, Orange notified the CNIL that a software platform used to send promotional messages on behalf of Orange was hacked, resulting in the theft of the personal data of 1.3 million users. A CNIL investigation found that Orange had not adequately audited the platform (an audit would have revealed potential security risks), had not applied security measures to emails sent to users and had failed to require its service provider processors to pass security obligations on to sub-contractors. The CNIL chose the sanction of a warning and, unusually, made the warning public on the basis that Orange was a large company with the scale of financial and human resources that should have allowed security issues to have been more adequately managed.

[CNIL article – 25 August 2014](#)

International

US

FTC Consults on Proposed Verifiable Parental Consent Method under COPPA

The Federal Trade Commission (FTC) is consulting on whether to approve a proposed verifiable parental consent method under the Children's Online Privacy Protection Act (COPPA), submitted for approval by AgeCheq, Inc. The Act requires websites to obtain parental permission before collecting personal data from a child. It sets out a number of approved methods of doing this but also allows third parties to submit other different methods for approval. The public has until 30 September 2014 to submit comments.

[CNIL article – August 2014](#)

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

Mark Gleeson

Partner

T +44 20 7655 1465

E mark.gleeson@squirepb.com

Stéphanie Faber

Of Counsel

T +33 1 5383 7400

E stephanie.faber@squirepb.com

Caroline Egan

Consultant

T +44 121 222 3386

E caroline.egan@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.