RegulatoryStrategies

UK Data Protection Newsletter January 2014

Headlines this month:

Commentary:

EU Data Protection Regulation deadline

Stakeholders have agreed on a new deadline for the adoption of EU Data Protection Regulation. This is now the end of 2014 allowing the 28 EU Member States to agree the remaining issues.

While progress has been described as 'painfully slow' by some stakeholders, the European Commission issued a press release entitled "Full Speed on EU Data Protection Reform". Viviane Reding, The EU's Justice Commissioner stated on the 27th January (ahead of Data Protection Day on 28th January):

"Data protection in the European Union is a fundamental right. Europe already has the highest level of data protection in the world. With the EU data protection reform which was proposed exactly two years ago - in January 2012 - Europe has the chance to make these rules a global gold standard. These rules will benefit citizens who want to be able to trust online services, and the small and medium sized businesses looking at a single market to more than 500 million consumers as an untapped opportunity. The European Parliament has led the way by voting overwhelmingly in favour of these rules. I wish to see full speed on data protection in 2014".

For further information contact Mike Bradford or Helen Lord at Regulatory Strategies
consultancy@regulatorystrategies.co.uk

Designed by Stolen Thunder Ltd.

© Copyright Regulatory Strategies Limited 2014. All rights reserved.

EU warns US about data protection

Vivian Reding has said that the EU-US "safe-harbor" agreement would be suspended if the US fails to take "legislative action before the summer". The EU Justice Commissioner has said that Safe Harbor needs to be repaired further to revelations about surveillance activities of the US National Security Agency.

The Commission has made 13 recommendations to improve aspects of improving Safe Harbor.

Breach trends

The ICO has updated its site to who the statistics for data breaches reported to them between April and December 2013. The update shows an increase of incidents with an increase of 25% being reported to the ICO in the third quarter than the first.

The health sector continues to report more incidents than any other sector. However, the Government requires NHS organisations to self-report data breaches. Local government, education, solicitors/ barristers and charities also featured among the sectors reporting the highest number of breaches.

Personal device at work policies

The ICO has promoted the need for organisations to have a clear policy about using personal devices at work. It recognises the benefits of people using their own devices in terms of efficiency, flexibility and employee morale. It also stresses there are associated risks.

The ICO's Group Manager (Technology) commented:

"AS the line between our personal wand working lives becomes increasingly blurred it is critical employers have a clear policy about personal devices being used at work.

"The benefits must be balanced against the potential risks to work-related personal data but the organisation should not underestimate the level of effort which may be required to ensure that the processing of personal data with BYOD remains compliant with all 8 Principles of the Data Protection act. Remember, it is the employer who is held liable for any breaches under the DPA."

The key recommendations are:

- **Ensure devices are secure:**
  - Ensure devices are locked with a strong password
  - Use encryption to store data securely
  - Separate private and work data
  - Devices should be approved for business use and separate apps should be used for personal use
- **Ensure data transfers are secure:**
  - Personal data transfers should be via a secure transfer
  - Care should be taken with untrusted connections e.g. open Wi-fi connections
  - Public cloud-based sharing and public backup services should be used and assessed with caution
- **Retain control:**
  - Devices should be registered with a remote locate and wipe facility
  - Users should know what data may be automatically or remotely deleted and under which circumstances
- **'End of contract' policy when an employee leaves or changes a device:**
  - Change the password and revoke access to facilities such as company email, intranet and social media
  - Provide information about how users should delete data prior to disposal, resale or recycling
- **Acceptable Use Policy:**
  - Implement and maintain and Acceptable Use Policy to provide guidance and accountability of behaviour
  - Consider if this needs to link to the Social Media Policy
  - Be clear about what type of personal data may be processed
  - Include all relevant departments

© Copyright Regulatory Strategies Limited 2014. All rights reserved.

GP practices

The ICO has issued a report showing positive approaches made by GP practices in protecting people's data. The report summarises 24 advisory visits undertaken by the ICO in the past year.

The visits showed surgeries tended to have good data protection practices and an awareness of issues. Security was generally good and procedures in place to protect data.

Areas for improvement included lack of awareness of the need to report data breaches, the need for improve the way patients are informed about how information would be used.

Credit default guidance

The ICO has withdrawn its guidance regarding "Filing defaults with credit reference agencies'. This reflects the ICO's approach to encourage industry to create its own guidance.

The 'Principles for the Reporting of Arrears, Arrangements and Defaults at Credit Reference Agencies' has now been drafted by the Steering Committee of Reciprocity (SCOR) which is made up of trade association, credit industry body and credit reference agency representatives.

Recent data protection breaches

ICU Investigations Limited

Six employees of ICU Investigations Limited were sentenced on 24th January 2014 for conspiring to breach the Data Protection Act. Five employees of the same company who had previously pleaded guilty were also sentenced.

ICU Investigations worked on behalf of other organisations to trace individuals primarily for the purposes of debt recovery. The company had checked utility companies, GP Surgeries and TV Licensing companies into releasing personal data.

Fines issued ranged between £1,000 and £4,000 against five individuals plus prosecution costs.

© Copyright Regulatory Strategies Limited 2014. All rights reserved.

EU update

The below provides an EU update from a Regulatory Strategies' partner, Newgate Public Relations, in Brussels, and provides an insight into the progress of the EU's draft data protection regulation:

RegulatoryStrategies

NEWGATE

www.newgatepr.com

General Data Protection reform

Last month the data protection reform was again high on the Brussels agenda whilst its creators and notably the EU politicians, were criticized for their hesitation in progressing the reform.

Paul Nemitz, the Director of the Fundamental Rights and Citizenship Directorate of the European Commission, has urged the ministers in charge to push the legislative package forward, arguing that there is no technical issue that could not be resolved. Even though it is not perfect, he said, it is important to have it approved in order to ensure legal certainty and send a strong political signal to the United Stated after the recent revelations about surveillance of, amongst others, EU political leaders. He added that as long as the draft Regulation is not finished, the U.S. will increase pressure to include the date protection reform in the ongoing trade negotiations, which the EU does not favour at all.

Peter Hustinx, in the last speech of his mandate as a European Data Protection Supervisor, addressed himself to the German government and said that the new coalition should take the lead in pushing forward the reform of the EU rules on data protection:

"Germany claims a special responsibility and role in the area of data protection. The new German government can tackle this subject with the necessary drive and energy and thereby gain acceptance of the German position at the European level and lead Europe to a higher level of data protection. However, this will require a constructive and proactive approach in the European debate."

A stronger opinion was expressed by Wojciech Wiewiorowski, the head of the Polish Data Protection Authority, who blamed the Commission for not defending its draft during the negotiations with the Council. Due to the fact that the Commission had failed to explain to the Council precisely what had to be achieved, Wiewiorowski feared the package could not be adopted before April. He said some Member States, such as Poland, were previously favourable to the Regulation though now they are withdrawing their support.

EU justice commissioner Viviane Reding, the European Parliament led negotiators on the package, the Greek EU presidency and the incoming Italian EU presidency concluded a political agreement to set the deadline until before the end of the year.

As the Greek Minister of Justice Athanasios pointed out in the Civil Liberties Committee on 21 January:

"The Hellenic presidency will intensify its efforts on this package, there are at least 20 meetings scheduled at technical level. There is no doubt that this is a highly political issue. The public opinion is sensitized in our Member States. The protection of personal data has to be adequate. The Hellenic presidency has raised this topic at the informal Council meeting the day after tomorrow in Athens, and we will continue this on a technical and political level."

For further information contact Mike Bradford or Helen Lord at Regulatory Strategies
consultancy@regulatorystrategies.co.uk

Designed by Stolen Thunder Ltd.

© Copyright Regulatory Strategies Limited 2014. All rights reserved.

The rather vague wordings of the Greek presidency did not reveal any precise commitments regarding timing yet indicate how politically delicate this reform is: in fact, Member states still have to reach a general approach before kicking off negotiations with the European Parliament and the European Commission.

Originally, the Parliament and the Commission had hoped to get the package adopted before the European elections in May. But with the announced delay, deputies will now have to vote to start the formal negotiations with Member States at the plenary session either in March or in April.

EU insiders are hoping the Member States will at least reach a partial approach in March and then a full agreement over the summer.

Among the core group of Member States willing to slow down the pace of the adoption process are the UK, Denmark, Hungary and Slovenia. All four are pushing to convert the Regulation, as it is actually on the table, into a less prescriptive Directive, leaving more room for manoeuvre for Member States.

Businesses have still time and opportunity to make their voice heard especially with Member States before the Institutions will enter into further negotiations.

Visit our website at www.regulatorystrategies.co.uk

For further information contact Mike Bradford or Helen Lord at Regulatory Strategies
consultancy@regulatorystrategies.co.uk

Designed by
Stolen Thunder Ltd.

© Copyright Regulatory Strategies Limited 2014. All rights reserved.