www.pwclegal.co.uk

Privacy and Security Enforcement Tracker 2014

March 2015

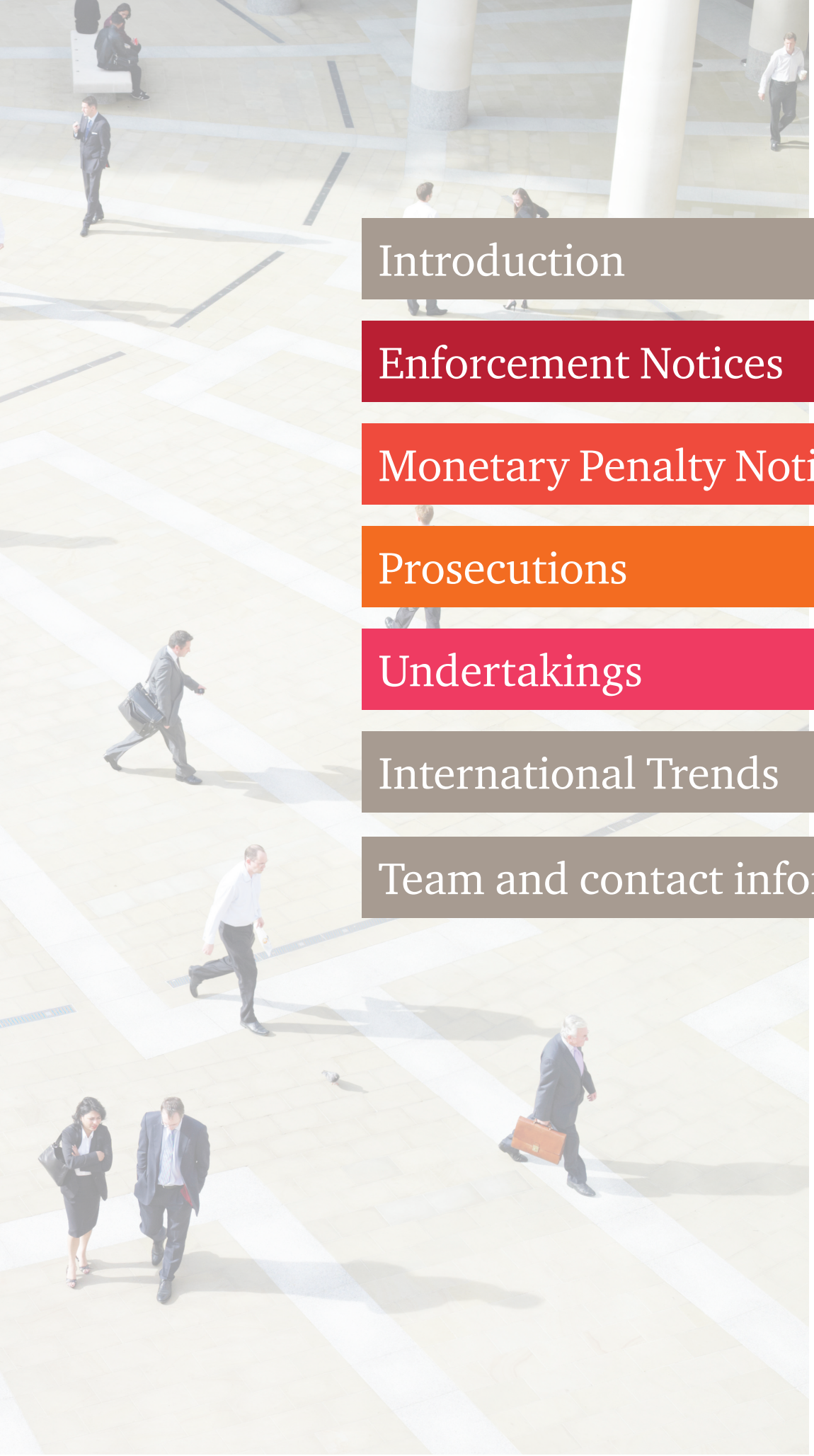
pwc

PricewaterhouseCoopers Legal LLP

A Look To The Future: Top 10 Emerging Regulatory Trends

Here are some of the influential opinions, guidelines, legal developments and news items in 2014. Whilst these items were not part of regulatory enforcement actions in 2014, and do not constitute an exhaustive list, ignore them at your peril. We predict that they will have a significant impact on businesses and the structure of the data protection, privacy and security enforcement landscape in 2015 and beyond:

1. February - ICO publishes PIA Code of Practice.
2. March – European Parliament votes to adopt the General Data Protection Regulation.
3. May - CJEU judgment in Google Spain case, on the so-called 'right to be forgotten'.
4. May - ICO report on online security vulnerabilities.
5. June - Irish High Court refers the Max Schrems case against Facebook to the CJEU.
6. July - ICO issues warning about wearables.
7. September - Article 29 Working Party opinion 8/2014 on Internet of Things.
8. October - Global Cross Border Enforcement Cooperation Arrangement published.
9. October – UK government mandates Cyber Essentials for its suppliers.
10. November - Article 29 Working Party opinion 9/2014 on device fingerprinting.



2014: The year of citizen, regulator and judicial activism

Welcome to the PwC Legal/ PwC Enforcement Tracker, our review of the critical data privacy and security regulatory enforcement cases in 2014.

2014 may be remembered as the year when citizen, regulator and judicial activists combined together to change the legal environment for privacy and security forever. In Europe, the biggest cases were Digital Rights Ireland and Google Spain, which unpicked the established positions on communications data retention and web search. In both of these cases, citizens and regulators pushed their cases to the Court of Justice of the European Union, an activist court, delivering outcomes that few commentators would have predicted in 2013. 2014 also saw citizen activists taking the UK government to court over the Prism and Tempora surveillance programmes and a related challenge to the EU/US Safe Harbour data transfer scheme, in litigation brought by a citizen activist against Facebook. The Prism/Tempora litigation reached a preliminary conclusion in early February this year, with a finding that the surveillance programmes were unlawful. All eyes are now on the Safe Harbour/ Facebook litigation, which has the capacity to cause chaos in EU/US business relationships.

Another major activist trend in 2014 was the rapid convergence in regulator cooperative working. The Global Privacy Enforcement Network (GPEN) continued to sign-up new national regulators, like the US Federal Communications Commission, and it even launched a website to trumpet its work, as well as creating an official contractual framework for its combined efforts. Regulators in the Commonwealth created the 'Common Thread Network'. The 'Mobile App Sweep' in autumn 2014 was one of a number of high profile cooperative outputs. Clearly, the privacy and security regulators want to leave the impression that there are no safe havens from global regulation.

Our Enforcement Tracker focuses on more parochial issues however, namely the way that privacy and security law is enforced on the ground, by national regulators. While national enforcement cases may lack the glitz and glamour of the famous international cases, their power to shape the environment is probably unrivalled. If you are an advisor to business, as PwC Legal and PwC are, you cannot afford to lose sight of the developments on the ground. If you are a regulated entity, a failure to track and react to developments can cause you massive business disruption. Quite simply, if you are a regulated entity you need to be able to adjust your business operations to take account of current and emerging regulatory activities. National regulators are the kings of the privacy and security world.

49% of PwC clients have a cyber-security policy that is updated in line with regulatory changes and enforcement cases.

(Source: Legal Business, Anatomy of a breach, PwC Insight Report)

This year the main focus of our Tracker is the UK and the enforcement activities of the Information Commissioner, but we have been joined by some of our colleagues abroad, who have provided snap shot pictures of the key developments in their jurisdictions in 2014. The 2015 Tracker, which will be published in early 2016, promises to be a much bigger international affair.

So, back to the UK; what are the key messages from 2014? Well, it is clear that that ICO is taking a more rounded view to the use of its enforcement powers. There has been a marked shift away from attention-grabbing financial penalties, to more subtle – and some might say more effective – enforcement tools, namely Enforcement Notices and Undertakings. However, the enforcement output has remained fairly constant over the past three years in terms of the volume of concluded cases. In other words, the ICO remains as busy as ever.

28% of PwC clients see cyber security as a board-level issue for their business.

(Source: Legal Business, Anatomy of a breach, PwC Insight Report)

The main reason for enforcement action in the UK remains security breaches, so we encourage readers to prioritise security over everything else. Cyber Security is clearly a new regulatory priority. But we also see a new contender for enforcement action, namely direct marketing offences. In our view, the focus on cold calling and the quality of direct marketing consents resembles the initial focus on data security back in 2006, which ramped up to a fining frenzy in 2012. We are telling our clients to track these developments closely, because in a few years' time we are bound to see a much stronger enforcement environment for all activities connected with the monetisation of the customer, particularly any forms of advertising that rely on customer data or customer insights.

In a more practical sense, we are encouraging our clients to move away from a 'legalistic' approach to legal compliance. Regulators are now focused on the operational realities of compliance, not the legislative headlines. The compliance obligation requires the delivery of operational change, not simply the creation of policy frameworks, contracts and other documentation. Risks need to be properly identified, their impacts properly assessed and the solutions properly designed. This requires a multi-disciplinary approach to compliance, which PwC Legal and PwC are critically placed to achieve.

If you want further information about how we can help you, please make contact with any member of our team. In London we hold monthly Privacy and Security Breakfast Briefings, to help our clients and contacts deliver meaningful and measurable operational change, but if you want to keep updated at a distance, please visit our blog at pwc.blogs.com/data_protection/. If you have suffered a security or personal data breach and you need help, please consider our Breach Aid service, which you can find more information about at www.pwc.co.uk/en_UK/uk/breach-aid/index.html.

Stewart Room
Partner
Global Head of Cyber Security and Data Protection
PwC Legal
+44 (0) 20 7213 4306
stewart.room@pwclegal.co.uk
@StewartRoom

Helpline calls received by ICO:

2010/2011
192,212

2011/2012
207,114

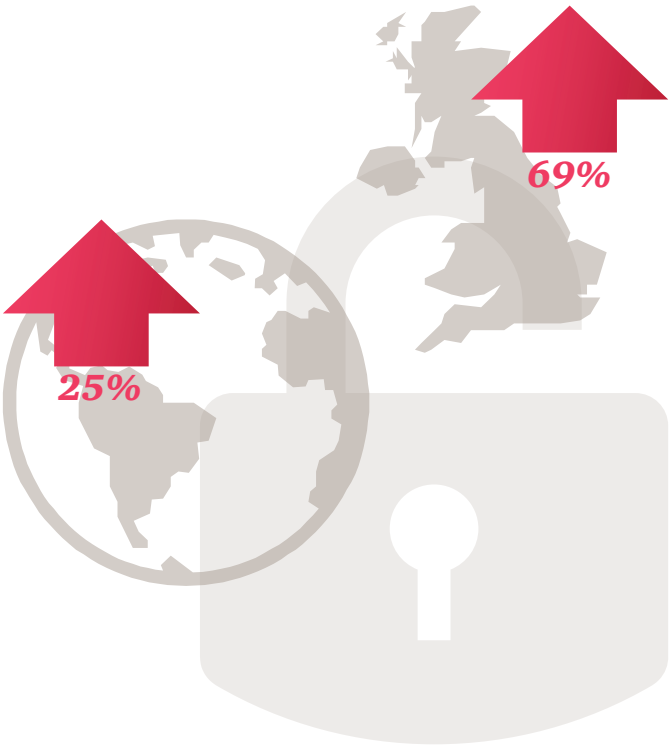
2012/2013
225,138

2013/2014
259,903

2014/2015
Another record year?

(Source: *Information Commissioner's Annual Report and Financial Statements 2013/2014, Effective, efficient – and busier than ever,* July 2014)

Security incident trends in 2014



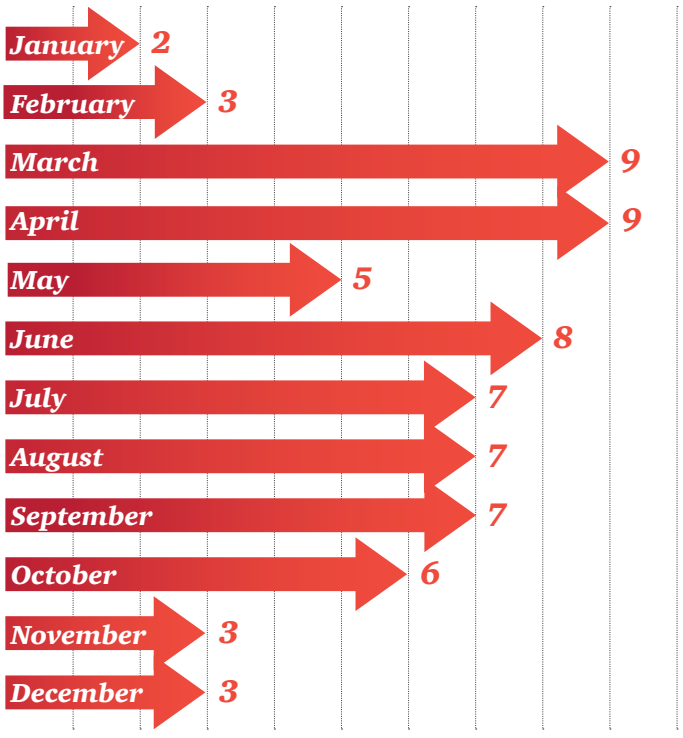
The number of security incidents detected in the UK in the past year increased by 69%, compared to a global increase of just 25% (Source: PwC, *The Global State of Information Security Survey 2015,* 30 September 2014)

Enforcement activities in 2014 by sector

Enforcement in the UK: comparing 2014, 2013 and 2012

	Monetary Penalty Notices	Prosecutions	Emforcement Notices	Undertakings	Total
2012	25	6	3	31	65
2013	18	7	7	22	54
2014	11	18	11	29	69

ICO enforcement actions in 2014 by month



Enforcement Notices

Total	***11***
Public Sector	***2***
Private Sector	***9***

Isisbyte Limited

10 March 2014

No fine

PEC Regulations – Regulation 24

ICO received complaints via the Telephone Preference Service (TPS) that various individuals acting on behalf of Isisbyte made unsolicited marketing calls to promote the company's goods and services. The callers did not provide Isisbyte's name or the company on whose behalf the calls were made.

Enforced remedial action required within 35 days:

1. Isisbyte must stop using a public communications services for direct marketing purposes unless they provide a name of the person calling and either an address or telephone number on which the caller can be reached free of charge.

SLM Connect Limited

10 March 2014

No fine

PEC Regulations – Regulation 24

ICO received complaints via the TPS that various individuals acting on behalf of SLM made unsolicited marketing calls to promote the company's goods and services. The callers did not provide SLM's name or the company on whose behalf the calls were made.

Enforced remedial action required within 35 days:

1. SLM must stop using public communications services for direct marketing purposes and automated calls, unless they provide a name of the person calling and either an address or telephone number on which the caller can be reached free of charge.

Amber UPVC Fabrications Limited

1 April 2014

Fine on 3 April 2014 of £50,000

PEC Regulations – Regulation 21

Amber UPVC made unsolicited calls to recipients who had registered themselves with the TPS and/or people who had not consented to them calling. They ignored warnings in several correspondences with ICO that their actions were unlawful and could attract a penalty.

Enforced remedial action required within 35 days:

1. Amber UPVC must stop public electronic communications services for the purpose of making unsolicited calls for direct marketing where the called line is that of:
   i. a subscriber who has previously notified Amber UPVC that calls should not be made on that line; and/or
   ii. a subscriber who has registered with the TPS at least 28 days previously and who has not notified Amber UPVC that they do not object to calls being made.

Wolverhampton City Council

15 May 2014

No fine

DPA – 7th principle

A data breach at the council occurred in January 2012. A social worker, who had not received data protection training, sent out a report to a former service user detailing their time in care. However, the social worker failed to remove highly sensitive information about the recipient's sister who had no right to see that information.

Enforced remedial action required within 50 days:

1. The council is required to ensure that all staff have completed the 'Protecting Information' e-learning module.

9/11

Enforcement Notices issued in 2014 were for direct marketing breaches of PECR

Only ***1***

Enforcement Notice and Monetary Penalty Notice combination (Amber UPVC Fabrications Limited)

DC Marketing Limited

10 June 2014

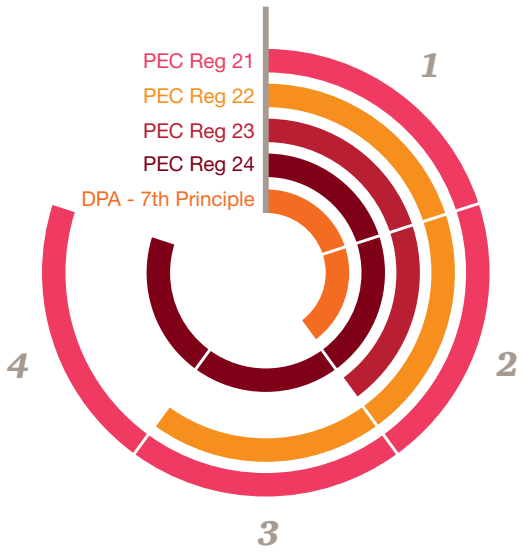
No fine

PEC Regulations – Regulations 21 and 24

ICO received numerous complaints via the TPS about DC Marketing Limited, who made hundreds of unsolicited marketing calls to try and get people to purchase solar panels partly financed by the Green Deal Home Improvement Fund. The complainants had told the company not to call again and/or were registered with the TPS, but despite this the complainants continued to receive calls from the company. An ICO investigation found the company also frequently gave a false name to avoid detection.

Enforced remedial action required within 35 days:

1. Neither use nor instigate a public electronic communications service to make unsolicited calls for direct marketing purposes where the called line is that of:
   i. a subscriber who has previously told DC Marketing Limited that calls should not be made; and/or
   ii. a subscriber who has registered their number with the TPS at least 28 days previously and who has not notified DC Marketing Limited that they do not object to such calls being made.
2. Cease using a public communications service for the transmission of a communication to people who have previously notified DC Marketing Limited that such calls should not be made on that line or if the number is listed with OFCOM unless DC Marketing Limited can provide a name of the person calling and either an address or telephone number on which the caller can be reached free of charge.



Breach summary - reasons for Enforcement Notices in 2014

Winchester and Deakin Limited

27 August 2014

No fine

PEC Regulations – Regulations 21 and 24

Winchester and Deakin Limited (also trading as Rapid Legal and Scarlet Reclaim) made unsolicited marketing calls to people who had registered with the TPS or who had asked not to be contacted. Complainants allege that they continued to receive calls despite complaining to ICO and/or the TPS.

Enforced remedial action required within 35 days:

1. Neither use nor instigate a public electronic communications service to make unsolicited calls for direct marketing purposes where the called line is that of:
   i. a subscriber who has previously told Winchester and Deakin Limited that calls should not be made; and/or
   ii. a subscriber who has registered their number with the TPS at least 28 days previously and who has not notified Winchester and Deakin Limited that they do not object to such calls being made.
2. Cease using a public communications service for the transmission of a communication to people who have previously notified DC Marketing Limited that such calls should not be made on that line or if the number is listed with OFCOM unless DC Marketing Limited can provide a name of the person calling and either an address or telephone number on which the caller can be reached free of charge.

Hot House Roof Company Limited

2 September 2014

No fine

PEC Regulations – Regulation 21

ICO has received numerous complaints from individuals who alleged that they received unsolicited marketing calls from various individuals acting on behalf of Hot House Roof Company Limited marketing its goods and services. Each complainant stated that they notified the company that such calls should not be made and/or that they had registered with the TPS. Despite this, many complainants reported that they continued to receive such calls.

Enforced remedial action required within 35 days:

1. Hot House Roof Company Limited must stop public electronic communications services for the purpose of making unsolicited calls for direct marketing where the called line is that of:
   i. a subscriber who has previously notified Hot House Roof Company Limited that calls should not be made on that line; and/or
   ii. a subscriber who has registered with the TPS at least 28 days previously and who has not notified Hot House Roof Company Limited that they do not object to calls being made.

All Claims Marketing Limited

8 September 2014

No fine

PEC Regulations – Regulations 22 and 23

All Claims Marketing Limited sent millions of unsolicited marketing text messages to individuals who had not given their prior consent, without providing information as to the identity of the person on whose behalf the communications had been sent.

Enforced remedial action required within 35 days:

1. Unless All Claims Marketing Limited has obtained contact details in the course of a sale or the marketing is related to similar products/services; and there is an option to refuse direct marketing, All Claims Marketing Limited cannot instigate or transmit unsolicited electronic direct marketing communications unless the recipient has notified All Claims Marketing Limited that he consents.
2. Not to transmit or instigate electronic direct marketing communications unless All Claims Marketing Limited is clearly identified as the sender

Abdul Tayub

10 October 2014

No fine

PEC Regulations – Regulations 22 and 23

Abdul Tayub was found to be sending unsolicited marketing mail by electronic means without providing information as to his identity and without prior consent.

Enforced remedial action required within 35 days:

1. Unless Abdul Tayab has obtained contact details in the course of a sale or the marketing is related to similar products/services; and there is an option to refuse direct marketing, Abdul Tayab cannot instigate or transmit unsolicited electronic direct marketing communications unless the recipient has notified Abdul Tayab that he consents.
2. Not to transmit or instigate electronic direct marketing communications unless Abdul Tayab is clearly identified as the sender

Grampian Health Board

18 November 2014

No fine

DPA – 7th principle

The ICO was informed that there were 6 separate incidents in a 13 month period where documents containing personal data were discovered in a number of public areas of the hospital, and on one occasion in a supermarket. ICO found that a number of recommendations following an audit in 2012 were still to be completed.

Enforced remedial action required:

1. By 22 June 2015 produce an overarching high level information asset register assigning owners.
2. By 31 March 2015 provide ICO with a progress report on compliance with step 1.
3. By 29 June 2015 confirm to ICO that step 1 has been complied with.

Optical Express (Westfield) Limited

19 December 2014

No fine

PEC Regulations – Regulation 22

Over a period of seven months between 10 September 2013 and 1 April 2014, over 4,600 complaints were made to ICO about Optical Express. The complainants reported that, despite having registered with the TPS, they had received unsolicited marketing text messages which included details about a competition to win laser eye surgery.

Enforced remedial action required within 35 days:

1. Unless Optical Express has obtained contact details of the recipient in the course of a sale, the directing marketing is in respect of similar products/services only and there is an option to refuse direct marketing, Optical Express must not send unsolicited direct marketing text messages unless the recipient has notified Optical Express that he consents.

4

Instances where Enforcement Notice was issued for breaching more than one PEC Regulation

Enforced remedial action was required within **35** days for over **80%** of Enforcement Notices

Monetary Penalty Notices

Total	***11***
Private Sector	***7***
Public Sector	***3***
Charities	***1***
Total Value	***£1,152,500***

Department of Justice Northern Ireland

14 January 2014

£185,000

DPA – 7th principle

Compensation Agency Northern Ireland (CANI), an agency dealing with compensation claims arising out of terrorist incidents in Northern Ireland, moved offices and sold a filing cabinet at an auction without checking its contents. The filing cabinet contained highly personal and sensitive details about victims of terrorist attacks, injuries suffered and family details.

Aggravating factors:

1. Behavioural issues – three other 'near misses' arising out of the office move.
2. Impact on CANI - sufficient financial resources to pay a monetary penalty without causing undue financial hardship; liability does not fall on any one individual.

Mitigating factors:

1. Effect of contravention – no evidence the data has been further disseminated.
2. Behavioural issues – remedial action now taken; full cooperation with ICO; full investigation carried out.
3. Impact on CANI – significant impact on reputation of data controller; liability to pay monetary penalty will fall on public purse although the penalty will be paid into Consolidated Fund.

Remedial Action:

1. Detailed procedures for removal of items (such as: cupboards, pedestals and filing cabinets etc.) from one office location to another to ensure any personal data contained in such furniture will be disposed of promptly and securely.

British Pregnancy Advice Service (BPAS)

28 February 2014

£200,000

DPA – 7th principle

An individual opposed to abortion hacked the BPAS website obtaining the details of nearly 10,000 individuals who had registered their contact details to request a call back for advice. The website offers advice on matters including: contraception, STI screening, abortion and erectile dysfunction – individuals whose details were obtained were likely to be seeking advice about these issues.

Aggravating factors:

1. Impact on BPAS – sufficient financial resources to pay a monetary penalty up to the maximum without causing undue financial hardship.
2. Effect of contravention – some individuals' ethnicity and social backgrounds could have led to physical harm or even death if the information had been disclosed.

Mitigating factors:

1. Nature of the contravention – attacked by a criminal who was convicted under the Computer Misuse Act 1990.
2. Effect of the contravention – injunction to prevent publication obtained within 12 hours; the details have not been further disseminated.
3. Behavioural issues – voluntarily reported to ICO; full co-operation with ICO; remedial action now taken .
4. Impact on BPAS – registered charity and provides services on behalf of the NHS; significant impact on reputation; the breach was publicised in the media.

Remedial Action:

1. BPAS has removed call back details from the website.
2. Substantial remedial action to ensure the breach will not be repeated.

Common aggravating features leading to higher fines:

- Minimal engagement with ICO
- Liability not falling on one individual
- Significant financial resources
- Particularly sensitive and confidential data

Common mitigating features leading to reduced fines:

- Co-operation with ICO
- Voluntary reporting to ICO
- Swift remedial action
- Subject to concerted criminal attack
- Data not used or further disseminated
- Liability to pay monetary penalty will fall on the public purse

Chief Constable of Kent Police

17 March 2014

£100,000

DPA – 7th principle

Confidential and highly sensitive personal information was left in a box at the site of a former police station. The items in the box included information about: murder threats; rape; grievous bodily harm; child abuse; interviews with victims, witnesses and informants; and police staff pay.

Aggravating factors:

1. Impact on Kent Police - sufficient financial resources to pay a monetary penalty without causing undue financial hardship; liability does not fall on any one individual.

Mitigating factors:

1. Effect of contravention – no evidence information has been further disseminated.
2. Behavioural issues – remedial action has been taken; full co-operation with ICO.
3. Impact on Kent Police – significant impact on the reputation of the data controller; liability to pay a monetary penalty will fall on the public purse although the penalty will be paid into a Consolidated Fund.

Remedial Action:

1. Procedure has been implemented to be followed when vacating police premises.

decline in the number of MPNs issued in 2014 compared to 2012.

Amber UPVC Fabrications Limited

1 April 2014

£50,000

PEC Regulations – Regulation 21

Amber UPVC made unsolicited calls to recipients who had registered themselves with the TPS, ignoring warnings in several correspondences with ICO that their actions were unlawful and could attract a penalty.

Aggravating factors:

1. Nature of the contravention – despite instructing the caller not to call the complainants continued to receive them; on-going contravention of PECR since 2006; no signs controls implemented since 2011 have worked.
2. Effect of contravention – large number affected by calls.
3. Behavioural issues – limited engagement with ICO; Amber UPVC failed to respond on 377/511 times when contacted by ICO; not changing its practices shows a complete disregard for PECR; no reasonable steps taken to comply with PECR during period of complaint.
4. Impact on Amber UPVC - private organisation within competitive industry and continuous breaches of PECR could create an unfair advantage.

Mitigating factors:

1. Nature of contravention – Amber UPVC may have believed the numbers it was using belonged to people who had consented to receive calls.
2. Behavioural issues – no evidence calls made were of an aggressive nature.
3. Impact on Amber UPVC – sufficient financial resources to pay penalty proposed without undue financial hardship; potential for damage to reputation that may affect future business.

Remedial Action:

1. No clear remedial action.

of legal teams are heavily involved in the drafting and review of security and contractual framework policies.

(Source: Legal Business, Anatomy of a breach, PwC Insight Report)

Think W3 Limited (TW3)

21 July 2014

£150,000

DPA – 7th principle

A vulnerability in the coding on TW3's website allowed a hacker to use a SQL injection attack to extract over one million credit and debit card details. Although CVV numbers were not stored, the hacker gained access to information including: customer names, addresses, postcodes, telephone numbers and email addresses.

Aggravating factors:

1. Impact on TW3 – limited company so liability to pay monetary penalty will not fall on any individual; sufficient financial resources to pay a monetary penalty without causing undue financial hardship.

Mitigating factors:

1. Nature of the contravention – subject to a criminal attack; ICO not aware of a previous similar breach.
2. Effect of contravention – no evidence personal data has been used for fraudulent transactions.
3. Behavioural issues – voluntarily reported to ICO; co-operation with ICO; website promptly locked down when breach was discovered; website system updated sooner than had been planned as a result of the breach; already in a tokenisation program to improve data security.
4. Impact on TW3 – significant impact on reputation of data controller as a result of the security breach.

Remedial Action:

1. Prompt remedial action to lock down relevant website; systems and web server to prevent further disclosure of data.

Reactiv Media Limited (RML)

24 July 2014

£50,000

PEC Regulations – Regulation 21

RML made 601 unsolicited marketing calls to members of the public who had registered with the TPS, despite evidence suggesting RML were aware they were in breach of Regulation 21. In December 2012 RML was ranked in the TPS Top 20 for the most complained about organisations.

Aggravating factors:

1. Nature of contravention – despite informing caller not to call again they continued to do so; RML failed to provide adequate company information.
2. Effect of contravention – repeated invasions of privacy; individuals deprived of rights under DPA/PECR.
3. Behavioural issues – minimal engagement with ICO; no requested information provided.
4. Impact on RML - private organisation within competitive direct marketing industry and continuous breaches of PECR could create an unfair advantage.

Mitigating factors:

1. Behavioural issues – there is evidence of some engagement with the TPS; RML has not featured in the TPS Top 20 since October 2013.
2. Impact on RML – potential for damage to reputation of RML which may affect future business.

Remedial Action:

1. No mention of remedial action.

30% of MPNs issued as a result of cyber-attacks, compared with **0%** in 2012.

Respondents to PwC's 2015 Global State of Information Security Survey reported a 41% jump in cyber security incidents.

(Source: PwC, *The Global State of Information Security Survey 2015*, 30 September 2014)

Ministry of Justice

20 August 2014

£180,000

DPA – 7th principle

An unencrypted hard drive containing information on 2,935 prisoners was lost and has not been recovered. The hard drive had not been locked in a safe as required. The information included: names, length of sentences, dates of birth, physical descriptions, intelligence leading to organised crime and victim details.

Aggravating factors:

1. Nature of the contravention – particularly serious due to the highly confidential and sensitive nature of the data.
2. Behavioural issues – failure to take effective remedial action following a similar breach in October 2011.
3. Impact on Ministry of Justice - sufficient financial resources to pay a monetary penalty without causing undue financial hardship.

Mitigating factors:

1. Nature of contravention – no evidence personal information has been disseminated; unencrypted hard drive should have been stored in a fireproof safe.
2. Behavioural issues – attempted remedial action in October 2011 but this was ineffective; breach was self-reported; full co-operation with ICO.
3. Impact on Ministry of Justice - significant impact on reputation; liability to pay monetary penalty will fall on public purse although the penalty will be paid into Consolidated Fund.

Remedial Action:

1. Encryption software for remaining hard drives was activated or upgraded.
2. New intelligence system has been implemented in all prisons removing need for manual back up.

Kwik Fix Plumbers Limited

22 September 2014

£90,000

PEC Regulations – Regulation 21

The ICO received a total of 214 complaints from individuals registered with the TPS who had been subjected to unsolicited direct marketing calls from Kwik Fix. Some of the complaints were made by or on behalf of vulnerable individuals, some of whom were sold boiler insurance they did not need. Kwik Fix were positioned at number 3 on the ICO's list of Top 20 most complained about organisations in November 2013.

Aggravating factors:

1. Nature of the contravention – calls made to the elderly and those suffering with Dementia/Alzheimer's; despite informing the caller not to call again they continued to do so; Kwik Fix failed to provide adequate company information.
2. Effect of contravention – repeated invasions of privacy and distress; individuals deprived of their rights under the DPA/PECR.
3. Behavioural issues – callers made false and misleading statements to persuade subscribers to purchase insurance unnecessarily.
4. Impact on Kwik Fix – private organisation within competitive direct marketing industry where continuous breaches of PECR could create unfair advantage.

Mitigating factors:

1. Behavioural issues – Kwik Fix has not featured in the TPS Top 20 since November 2013; evidence of some engagement with the TPS; guidance given to staff on making calls.
2. Impact on Kwik Fix – potential damage to reputation which may affect future business.

Remedial Action:

1. No clear remedial action.

MPNs issued for:

- inappropriate disposal of data (£285,000)
- cyber-attacks (£357,500)
- marketing calls (£260,000)
- marketing text messages (£70,000)
- unencrypted device (£180,000)

30%

of MPNs issued for direct marketing breaches of PECR

EMC Advisory Services Limited (EMCAS)

29 September 2014

£70,000

PEC Regulations – Regulation 21

EMCAS has been fined after the TPS and ICO received a total of 630 complaints about the company, after the complainants received unsolicited direct marketing calls despite having been registered with the TPS and/or having asked EMCAS not to call. EMCAS appeared in the TPS Top 20 most complained about organisations in May 2012.

Aggravating factors:

1. Nature of the contravention – complainants informed caller not to call again but this was ignored.
2. Effect of contravention – repeated invasions of privacy and distress.
3. Behavioural issues – no acceptance that they are instigator of calls made on EMCAS's behalf by 3rd parties.
4. Impact on EMCAS - private organisation within competitive direct marketing industry and continuous breaches of PECR could create an unfair advantage.

Mitigating factors:

1. Nature of contravention – EMCAS say they do screen against TPS.
2. Behavioural issues – full engagement with ICO; substantial remedial action now taken; compensation has been paid to complainants; complaints received by ICO and TPS has reduced.
3. Impact on EMCAS - potential for damage to reputation of EMCAS which may affect future business.

Remedial Action:

1. Nothing specific mentioned.

Worldview Limited

31 October 2014

£7,500

DPA – 7th principle

A vulnerability in Worldview's website code allowed a hacker to perform a blind SQL injection attack. The hacker gained access to full payment card details of 3,814 people, including encrypted card data and CVV numbers. Although the files were locked down when the breach was found, the hacker had access to the systems for up to 10 days.

Aggravating factors:

1. Impact on Worldview - limited company so liability to pay monetary penalty will not fall on any individual; sufficient financial resources to pay a monetary penalty without causing undue financial hardship.

Mitigating factors:

1. Nature of contravention – systems were subject to a criminal attack; online marketing administrator should have used a stronger password; no previous similar breach.
2. Effect of contravention – no evidence personal data has been used for fraudulent purposes.
3. Behavioural issues - voluntarily reported to ICO; full cooperation with ICO; offered compensation for any inconvenience suffered by individuals; remedial action now taken.
4. Impact on Worldview - significant impact on reputation Worldview.

Remedial Action:

1. Nothing specific mentioned

Total value of MPNs:

2014 - £1,152, 500

2013 - £1,520,000

2012 - £2,430,000

2011 - £541,000

Steady decline in MPNs issued over the course of 2012, 2013 and 2014

Parklife Manchester Limited

2 December 2014

£70,000

PEC Regulations – Regulation 23

Parklife Manchester Limited, the company behind the Parklife Weekender music festival, sent approximately 70,000 unsolicited marketing text messages to people who had bought tickets to the previous year's event. The text messages concealed the fact that Parklife Manchester Limited was the sender, as the messages appeared on the recipients' phones as sent by 'Mum' – this caused considerable distress for a variety of personal reasons.

Aggravating factors:

1. Nature of the contravention – 70,000 messages sent; no prior consent; failed to provide valid address to opt out of further marketing; recipients were generally young or vulnerable.
2. Effect of contravention – 76 people complained; many of the complainants suffered substantial distress.
3. Behavioural issues – the company did not initially take the complaints seriously as it tweeted: 'so this is what it feels like to be a jar of Marmite #LoveItOrHateIt'.

Mitigating factors:

1. Nature of the contravention – the contravention was a one off.
2. Behavioural issues – public statement eventually issued apologising for distress; full co-operation with ICO.
3. Impact on Parklife – damage to reputation of Parklife which may damage future business.

Remedial Action:

1. N/A

Number of MPNs:

2014 - 11

2013 - 18

2012 - 25

of PwC clients have an incident response plan, of which 40% require legal to be involved at an early stage.

(Source: Legal Business, *Anatomy of a breach*, PwC Insight Report)

Prosecutions

Total	***18***

ICU Investigations Limited

24 January 2014

ICU Investigations Limited worked on behalf of clients to trace individuals primarily for the purpose of debt recovery. The company routinely tricked utility companies into revealing personal data, often pertaining to the individuals they were trying to trace.

Sentence:

6 employees were fined a total of £18,500 and ordered to pay £15,607 prosecution costs.

Becoming Green (UK) Limited

11 March 2014

Becoming Green (UK) Limited, and the company's director Abdul Muhith, were prosecuted for failing to register with the ICO that the company handled customers' personal data.

Sentence:

Both were fined £270, ordered to pay a victim surcharge of £27 and ordered to pay costs of £300.

Boilershield Limited

12 March 2014

Boilershield Limited, and the company's director Mohammod Ali, were prosecuted for failing to register with the ICO that the company handled customers' personal data.

Sentence:

Both pleaded guilty and were fined £1,200, ordered to pay a victim surcharge of £120 and ordered to pay costs of £196.87.

Help Direct UK Limited

25 March 2014

Financial advisor Help Direct UK Limited was prosecuted for failing to register with the ICO that the company handled customers' personal data.

Sentence:

The company pleaded guilty and was fined £250, ordered to pay a victim surcharge of £25 and ordered to pay costs of £248.83

Barry Spencer

25 April 2014

Barry Spencer ran ICU Investigations Limited who worked on behalf of clients to trace individuals primarily for the purpose of debt recovery. The company routinely tricked utility companies into revealing personal data, often pertaining to the individuals they were trying to trace.

Sentence:

Spencer was found guilty under s55 DPA and was ordered to pay a £12,000 fine and £8,000 towards prosecution costs. A confiscation order of £69,327.32 was made under the Proceeds of Crime Act and Spencer was threatened with a 20 month prison sentence if it was not paid.

Allied Union Limited

25 April 2014

Pension review company Allied Union Limited was prosecuted for failing to register with the ICO that the company handled customers' personal data.

Sentence:

The company pleaded guilty and was fined £400, ordered to pay a victim surcharge of £40 and ordered to pay costs of £338.11.

QR Lettings

13 May 2014

Property company QR Lettings was prosecuted for failing to register with the ICO that the company handled customers' personal data.

Sentence:

The company pleaded guilty and was fined £250, ordered to pay a victim surcharge of £30 and ordered to pay costs of £260.

The number of prosecutions in 2014 ***tripled*** compared to 2012.

API Telecom

5 June 2014

Telecoms company API Telecom was prosecuted for failing to comply with an information notice.

Sentence:

The company pleaded guilty and was fined £200, ordered to pay a victim surcharge and ordered to pay full costs of £489.85.

Darren Anthony Bott (a director of Allied Union Limited)

6 June 2014

Darren Anthony Bott, a director of Allied Union Limited, was prosecuted for failing to notify with the ICO.

Sentence:

Bott pleaded guilty and was fined £400, ordered to pay a victim surcharge of £40 and ordered to pay costs of £218.82.

Global Immigration Consultants Limited

9 July 2014

Legal advice company Global Immigration Consultants Limited was prosecuted for failing to register with the ICO that it handled customers' personal data.

Sentence:

The company pleaded guilty and was fined £300, ordered to pay a victim surcharge of £30 and ordered to pay costs of £260.18.

Stephen Siddell (former branch manager of Enterprise Rent-A-Car)

10 July 2014

Stephen Siddell was a former branch manager at Enterprise Rent-A-Car who was prosecuted for unlawfully stealing the records of approximately two thousand customers in order to sell them to a claims management company.

Sentence:

Siddell was fined £500, ordered to pay a victim surcharge of £50 and ordered to pay costs of £264.08.

58% of prosecutions were for failing to notify the ICO under s17 DPA in 2014, compared to **50%** in 2012.

Hayden Nash Consultants

14 July 2014

Recruitment company Hayden Nash Consultants was prosecuted for failing to register with the ICO that it handled customers' personal data.

Sentence:

The company pleaded guilty and was fined £200, ordered to pay a victim surcharge of £20 and ordered to pay costs of £489.85.

Jayesh Shah (owner of Vintels)

15 July 2014

Jayesh Shah, owner of marketing company Vintels, was prosecuted for failing to notify the ICO of changes to his notification.

Sentence:

Shah was fined £4,000, ordered to pay a victim surcharge of £400 and ordered to pay costs of £2,703.

1st Choice Properties (SRAL)

5 August 2014

Property lettings and management company 1st Choice Properties (SRAL) was prosecuted for failing to register with the ICO that it handled customers' personal data.

Sentence:

The company was convicted in its absence and fined £500, ordered to pay a victim surcharge of £50 and ordered to pay costs of £815.08.

"The issues that most worry executives? The privacy of personal data, legal risks, and loss of intellectual property".

(Source: PwC, *The Global State of Information Security Survey 2015*, 30 September 2014).

A Plus Recruitment Limited

6 August 2014

Recruitment company A Plus Recruitment Limited was prosecuted for failing to register with the ICO that it handled customers' personal data.

Sentence:

The company pleaded guilty and was fined £300, ordered to pay a victim surcharge of £30 and ordered to pay costs of £489.95.

Dalvinder Singh (Santander UK suspicious activity reporting unit)

22 August 2014

Dalvinder Singh worked in Santander's suspicious activity reporting unit in Leicester. His role was to investigate money laundering activity at the bank, this gave him access to view customer accounts. In an abuse of this position he used his access to look at eleven colleagues' accounts to find information on their salaries and bonuses. This was a criminal offence as there was a clear violation of s55 DPA for unlawfully obtaining or accessing personal data.

Sentence:

Singh was fined £880, ordered to pay a victim surcharge of £88 and ordered to pay costs of £440.

Matthew Devlin

11 November 2014

Matthew Devlin has been prosecuted for illegally accessing one of Everything Everywhere's (EE) customer databases. He used the database to find out when EE customers were due an upgrade in order to target them with services offered by his own company. He impersonated an employee of Orange in an attempt to obtain customer passwords and login information, succeeding on one occasion in obtaining records relating to 1,066 customers.

Sentence:

Devlin was fined £500, ordered to pay a victim surcharge of £50 and ordered to pay costs of £438.63.

Harkanwarjit Dhanju

13 November 2014

Dhanju had responsibility for handling medication reviews for patients in local care homes with mental health issues. Whilst working as a sessional pharmacist at Tile House Surgery (part of the South West Essex Primary Care Trust) he used his security pass to unlawfully access the medical records of family members, work colleagues and local health professionals.

Sentence:

Dhanju was fined £1000, ordered to pay a victim surcharge of £100 and ordered to pay costs of £608.30.

Total number of prosecutions:

2014 - 18

2013 - 7

2012 - 6

Undertakings

Public vs private sectors	***22 public 7 private***
Total number of Undertakings in 2014	***29***
Follow up reports made in 2014 by ICO on Undertakings signed in 2013 and 2014	***18***

Northern Health & Social Care Trust

10 January 2014

DPA – 7th Principle

Northern Health & Social Care Trust has been involved in a number of incidents which have breached the DPA. The incidents included accidently faxing confidential service user information to a local business and making an inappropriate disclosure of minutes containing sensitive personal data to professionals working in partnership with the Trust.

The ICO investigation revealed that staff had not received what should have been mandatory Information Governance training.

Undertakings signed in August 2013:

1. Make staff aware of policy for storage and use of personal data.
2. Ensure staff attend mandatory training.
3. Ensure portable and mobile devices are encrypted to the required standard.
4. Put in place procedures to ensure prompt response to breach of security.
5. Ensure adequate security measures are in place to prevent unauthorised access to personal data.
6. Implement such other security measures as are appropriate to protect personal data.

Findings of ICO on 10 January 2014 in relation to Undertakings signed:

1. Extra training sessions organised.
2. Laptops and computers encrypted to the required standard.
3. End point security installed to prevent unencrypted USB media being used.
4. New procedure for reporting of Information Governance incidents.
5. The Trust has taken appropriate steps to address the requirements of the undertaking, but further steps are needed:
   i. Ensure Information Asset Owner's provide assurance to SIRO that procedures for storage of personal data are in place.
   ii. Review corporate induction materials in relation to Information Governance.
   iii. Review physical security measures where personal data is stored.
   iv. Finalise Processing of Personal Information Policy in terms of strengthening physical security of information and obtain input from the Trust Information Governance Forum.

Hillingdon Hospitals NHS Foundation Trust

24 January 2014

DPA – 7th Principle

A local newspaper ended up in possession of documents that should have been transferred via internal mail between The Hillingdon Hospital and Mount Vernon Hospital. It is unclear how the documents were lost or how the newspaper obtained possession.

It has been identified that there was a gap in the reporting mechanism for data protection incidents, as staff were aware documents had not arrived but the incident was not escalated.

Undertakings signed in September 2013:

1. Implement appropriate reporting mechanisms and make staff fully aware of reporting procedures and requirements.
2. Effectively manage escalation process if documents do not arrive at intended destination.
3. Implement such other measures as are deemed appropriate to ensure personal data is protected.

Findings of ICO on 24 January 2014 in relation to Undertakings signed:

1. There is now a documented process for prompt incident reporting.
2. The incident reporting process is covered within local induction and annual information governance training materials.
3. Improvement in security of patient information when transferred between sites, this included sealed packages and tracking of collection and delivery of documents.
4. In summary, the Trust has taken appropriate steps and put plans in place to address the undertaking requirements.

Approximately ***80%*** of Undertakings in 2014 were made by public sector organisations

Cardiff City Council

7 March 2014

DPA – 6th Principle

Following a request for assessment by a member of the public after the council failed to respond to a subject assess request within 40 days, ICO found that there were systemic failures in the council's compliance procedures.

Undertakings signed in August 2013:

1. Clearly define policies and procedures for dealing with subject access requests.
2. Staff involved with processing subject access requests should receive specialist training.
3. Designated staff to keep records of subject access requests received and responded to.
4. Put in place appropriate checks to ensure 3rd party data is dealt with in a way that is compliant with the DPA and the council's procedures.
5. Improvements to systems governing storage of paper records to ensure subject access requests are responded to in a timely manner.

Findings of ICO on 7 March 2014 in relation to Undertakings signed:

1. Policies and procedures relating to handling of subject access requests have been established.
2. Specialised training has been given to staff with responsibility for handling subject access requests.
3. Database of subject access requests received is operational.
4. Subject access request compliance information is regularly reported to senior management.
5. Quality assurance process is now in place to ensure 3rd party data is dealt with in accordance with DPA.
6. The council has taken appropriate steps to address the requirements of the undertaking, but further steps are needed:
    i. Ensure new EDRM system addresses the undertaking stipulation that improvements are made to systems governing storage of paper records, to ensure subject access requests are responded to in a timely manner.

Neath Care

13 March 2014

DPA – 7th Principle

Ten client care service delivery plans were found by a member of the public in the street. The delivery plans related to elderly people and contained confidential information such as personal care, medication and safe numbers.

There was a basic data protection policy in place however there was no clear procedure for safe handling and storage of sensitive personal data outside the office environment.

Undertakings:

1. By July 2014 implement a detailed policy for handling sensitive personal data outside the office environment.
2. By July 2014 implement a policy to ensure sensitive personal data taken outside the office is monitored, logged and returned.
3. Refresher training for all staff who handle personal data.
4. Implement such other security measures as are appropriate to comply with the DPA.

Findings of ICO in relation to Undertakings signed:

N/A

of GCs interviewed by PwC say that the legal department has assessed the extent to which the security of business operations is reliant on the services and operations provided by third parties.

(Source: Legal Business, Anatomy of a breach, PwC Insight Report)

Disclosure and Barring Service

20 March 2014

DPA – 1st Principle

Disclosure and Barring Service failed to amend e55 application forms after new legislation required it to do so when it came into force on 29 May 2013. Two individuals disclosed that they had minor criminal convictions/cautions which were seen by prospective employers who withdrew job offers. They would not have had to disclose such information if the e55 forms had been updated to reflect the current law.

Undertakings:

1. By 31 March 2014 the e55 form should be amended to include the question: 'do you have any convictions, cautions, reprimands or final warnings, which would not be filtered in line with the guidance?'.
2. By 31 July 2014 application form should include an insert giving applicants guidance on matters that will be filtered.
3. With immediate effect the supporting information given to applicants and employers is to be kept under review to ensure that they receive up to date and relevant guidance.

Findings of ICO in relation to Undertakings signed:

1. N/A

Barking, Havering & Redbridge University Hospitals NHS Trust (BHRUT)

28 March 2014

DPA – 7th Principle

A BHRUT employee sent faxes containing personal data to an incorrect fax number belonging to a member of the public. Despite the fact that Information Governance training was mandatory, the employee responsible had not received the training.

Undertakings:

1. Ensure that attendance at mandatory Information Governance training is enforced.
2. Maintain a full and accurate record of those who receive training.
3. Implement such other measures as are deemed appropriate to ensure personal data is protected.

Findings of ICO in relation to Undertakings signed:

1. N/A

Royal Borough of Windsor and Maidenhead

3 April 2014

DPA – 7th Principle

The details of 257 employees who had not signed a new employment contract were uploaded onto the intranet rather than being added as a restricted item as they should have been. This was a minor incident, but ICO discovered that policies and procedures on handling personal data were incomplete and that training was not a mandatory requirement.

Undertakings signed in September 2013:

1. By 31 December 2013 revise procedures for handling personal data, particularly in relation to information security.
2. By 31 December 2013 all staff to be made aware of policies and procedures for handling personal data.
3. By 31 December 2013 all staff whose roles involve handling personal data shall receive training.
4. Compliance with internal policies on data protection shall be monitored and enforced.
5. Implement such other security measures as are deemed appropriate to ensure personal data is protected.

Findings of ICO on 3 April 2014 in relation to Undertakings signed:

1. The council has revised procedures for handling personal data.
2. Introduced code of conduct and information handling policy is in development.
3. Ongoing training programme has been introduced.
4. Incident reporting, recording and investigation process has been introduced.
5. The Royal Borough has taken appropriate steps to address the requirements of the undertaking, but further steps are needed:
   i. Gain ratification for information handling policy.
   ii. Complete data protection training for all existing staff and new starters.

Great Ormond Street Hospital for Children NHS Trust (GOSH)

29 April 2014

DPA - 7th Principle

4 separate incidents in 18 months where letters containing medical information have been sent to the wrong address. The letters were sent by temporary or bank members of staff who had not received any relevant data protection training.

After investigating further, ICO discovered that there were a lack of policies and procedures in place to ensure accuracy of addresses.

Undertakings signed in November 2013:

1. Ensure temporary or bank staff are provided with sufficient data protection training.
2. Ensure data protection training is fully monitored and enforced.
3. Ensure sufficient processes are in place to ensure medical records and referral letters are sent to correct addresses.
4. Implement such other security measures as are appropriate to ensure personal data is protected.

Findings of ICO on 29 April 2014 in relation to Undertakings signed:

1. Information Governance training requirements for bank and temporary staff members have been reviewed.
2. Completion of 'Introduction to Information Governance' eLearning module is mandatory for all staff and is monitored.
3. Data illustrating compliance statistics are produced monthly.
4. Procedures for registration, outpatient and handling secure addresses have been updated.
5. Awareness campaign reminding patients' families to inform GOSH when their address changes was run.
6. In summary, the Trust has taken appropriate steps and put plans in place to address the undertaking requirements.

Panasonic UK

28 May 2014

DPA – 3rd and 7th Principles

An unencrypted laptop was stolen from an unlocked hotel room. The laptop contained names, addresses, contact details, dates of birth, passport details and emergency contact details of 970 people who had attended events arranged on Panasonic's behalf by a third party.

Panasonic does have comprehensive policies around data protection, but there is no evidence that the policies were communicated to the third party hosting Panasonic's events.

Undertakings signed in October 2013:

1. Ensure adequate contracts and checks are in place to comply with the DPA 7th Principle.
2. Ensure personal data collected is for a valid purpose and is not held longer than is necessary.
3. Implement such other security measures as are appropriate to ensure personal data is protected.

Findings of ICO on 28 May 2014 in relation to Undertakings signed:

1. New Data Processing Agreement template has been drafted.
2. Data Protection training has been improved.
3. Introduction of posters around the building to highlight importance of data protection.
4. Revised data privacy, data retention, cookies and personal information policies in place.
5. In summary, Panasonic has taken appropriate steps and put plans in place to address the undertaking requirements.

30%

of legal teams are involved in the design of policies, procedures and processes for the assessment of security in the supplier base.

(Source: Legal Business, Anatomy of a breach, PwC Insight Report)

St Helens Metropolitan Borough Council

30 May 2014

DPA – 7th Principle

Documents relating to a child in foster care were disclosed to the correct party. However, some of the information needed to be concealed and the address of a child's current foster placement was not redacted and was disclosed to the child's biological parents.

ICO established that there was no procedure in place for redaction of personal data and that there was no routine peer check on documents of this nature.

Undertakings:

1. Introduce a secondary peer review process prior to posting documents.
2. Provide advice to organisations who supply information to ensure personal information is removed prior to being received by the council.
3. Provide training and make staff aware of policies for storage and use of personal data.
4. Monitor compliance with these policies.
5. Implement such other security measures as are appropriate to ensure personal data is protected.

Findings of ICO in relation to Undertakings signed:

1. N/A

Jephson Homes Housing Association Ltd

2 June 2014

DPA – 7th Principle

Documents were disclosed to an individual as part of a litigation process containing personal data that should have been redacted but were instead disclosed in full.

Although there had been initial checks, there were no checks made immediately prior to the disclosure of the documents. Data protection training was provided to staff at induction but there was no refresher training in place.

Undertakings:

1. By 30 November 2014 provide guidance to staff about preparing information for disclosure.
2. By 30 November 2014 implement a process for checking and recording documentation prior to disclosure.
3. With effect from 30 November 2014 refresher data protection training for staff to be provided regularly.
4. Implement such other security measures as are appropriate to ensure personal data is protected.

Findings of ICO in relation to Undertakings signed:

1. N/A

More Undertakings this year than in 2013, but ***less*** than 2012

Worcestershire Health and Care NHS Trust

9 June 2014

DPA – 7th Principle

A patient handover sheet was handed to the press after it had been dropped in a waiting room at a train station by a temporary agency nurse. The list contained details relating to 18 patients concerning their medical conditions and treatment notes.

The incident uncovered wider information governance issues between the way permanent and temporary staff were offered data protection training. There was also no safe method for disposing of confidential waste.

Undertakings:

1. Communicate policies and guidance for disposal of confidential information to staff and install waste bins.
2. Permanent and agency staff should use consistent standards in relation to handling personal data.
3. Enforce completion of mandatory induction data protection training for both permanent and agency staff.
4. Implement such other security measures as are deemed appropriate to ensure personal data is protected.

Findings of ICO in relation to Undertakings signed:

1. N/A

Common themes in Undertakings:

- Requirements for mandatory staff training and refresher courses
- Training to be monitored and enforced
- Clear policies and guidelines communicated to staff
- Improvements to record keeping processes
- Incident reporting procedure improvements

Cardiff and Vale University Health Board

16 June 2014

DPA – 7th Principle

A consultant psychiatrist lost a bag containing sensitive personal data whilst cycling home from work. The sensitive personal data included: a mental health act tribunal report relating to a patient, a solicitor's letter, five CVs, a purse and a mobile phone.

In addition, Cardiff University Health Board was unable to demonstrate that mandatory data protection training was fully implemented.

Undertakings signed in October 2013:

1. Put in place an adequate security policy for the removal of documentation off site and while in transit. All staff should be made aware of this.
2. All data protection training should be made mandatory, completion of training is to be monitored and recorded.
3. Staff should be assessed for suitability for home working and secure methods of transporting relevant data.
4. Put in place a protective marking scheme and make use of redaction techniques where possible.
5. Compliance with data protection and IT security policies to be regularly monitored.
6. Implement such other security measures as are deemed appropriate to ensure personal data is protected.

Findings of ICO on 16 June 2014 in relation to Undertakings signed:

1. New policies for removal of documents off site and for security of data whilst in transit have been implemented.
2. NHS Wales has introduced mandatory Information governance training, this has been included into both corporate and local inductions.
3. The health board has taken steps to limit access to records on a 'need to know' basis.
4. The health board has introduced an Information Governance Investigation template to enable incidents to be reported and investigated properly.
5. In summary, the health board has taken appropriate steps and put plans in place to address the undertaking requirements.

Aberdeenshire Council

17 June 2014

DPA – 7th Principle

A social worker in the Adult Mental Health department lost a paper file containing sensitive information after leaving it on the roof of his car before driving off.

Although there was no evidence of unauthorised processing of the data, the social worker had not received any formal data protection training.

Undertakings:

1. By 15 October 2014 all staff who handle personal data should receive mandatory data protection training.
2. By 30 December 2015 set up a refresher data protection programme which should be updated at least every 3 years.
3. Attendance at data protection training sessions should be fully monitored.
4. Implement such other security measures as are deemed appropriate to ensure personal data is protected.

Findings of ICO in relation to Undertakings signed:

1. N/A

Betsi Cadwaladr University Health Board

9 July 2014

DPA – 7th Principle

8 letters concerning patients of the Health Board, 6 of which contained sensitive personal data, were sent to a patient in error instead of a GP surgery.

ICO found that the employee responsible had not received any formal data protection training.

Undertakings:

1. By 30 September 2014 all staff who handle sensitive information or whose role relates to information governance should receive data protection training.
2. By October 2015 all other staff who handle personal data should be trained.
3. All new staff should receive data protection training as part of induction.
4. Attendance on data protection training sessions is monitored and enforced.
5. Implement such other security measures as are appropriate to ensure personal data is protected.

Findings of ICO in relation to Undertakings signed:

1. N/A

The Moray Council

16 July 2014

DPA – 7th Principle

An employee left a bundle of papers containing sensitive personal data in a local café comprising detailed reports about the adoption of two children as well as information relating to 19 others.

ICO discovered that the employee signed an agreement stating that the documents would be kept in secure lock fast facilities. However, the council had not implemented supporting policies to advise staff how to keep personal data secure outside of an office environment and there was no compulsory training.

Undertakings signed in April 2014:

1. Implement a policy to ensure the security of personal data taken out of the office and inform staff of the policy.
2. Ensure data protection training is mandatory for staff handling personal data and ensure training is implemented across the council.
3. Review content of training to ensure it adequately covers loss of personal data.
4. Implement such other security measures as are appropriate to ensure personal data is protected.

Findings of ICO on 16 July 2014 in relation to Undertakings signed:

1. Undertakings 1-4 has been demonstrated as satisfied
2. The council has taken appropriate steps to address the requirements of the undertaking, but further steps are needed:
   i. Ensure training programme is rolled out to remainder of employees in the long term and that there refresher training.
   ii. Discuss data protection at operational levels and review information assurance on an annual basis.

53% of PwC clients would benefit from additional cyber security training or awareness. ***37%*** would like specific training on legal and regulatory standards.

(Source: Legal Business, Anatomy of a breach, PwC Insight Report)

Wokingham Borough Council

4 August 2014

DPA – 7th Principle

Subject access request documents went missing after they were delivered to the service user's home address and left on the doorstep. The documents contained sensitive personal data relating to the user and her children who had received help from social services following allegations of neglect and abuse by an ex-partner.

The incident occurred due to a failure in communication, as the courier was not given clear instructions not to leave the documents without obtaining a signature.

Undertakings signed in April 2014:

1. By 31 July make staff aware of policies and procedures for storage and use of personal data.
2. By 31 July training in data protection and information security to be given to all staff who handle personal data prior to accessing internal systems.
3. By 30 June 2014 procedures must be drafted to cover issues such as transporting paper records containing personal data outside an office environment.
4. Compliance with training on data protection to be regularly monitored and failings to be monitored and rectified.
5. Implement such other security measures as are deemed appropriate to ensure personal data is protected.

Findings of ICO on 4 August 2014 in relation to Undertakings signed:

1. Staff have completed data protection training.
2. New staff are required to complete training before gaining access to IT systems.
3. Guidance on transporting paper documents has been created.
4. Information Governance Group meets to implement a data protection work plan.
5. The Council has committed to reviewing and refreshing training material at regular intervals.
6. The council has taken appropriate steps to address the requirements of the undertaking, but further steps are needed:
   i. Undertaking requested that 'refresher training structure' should be implemented. This does not appear to be in place and action should be taken to implement this.

Undertakings: reasons for failure in 2014 (some incidents contain multiple failures)

Thamesview Estate Agents Ltd

11 August 2014

DPA – 7th Principle

The estate agent insecurely disposed of personal data in transparent refuse sacks left in the street whilst waiting for collection by a disposal company. In spite of a warning from ICO not to dispose of documents this way the estate agent continued to do so. The personal data included copies of passports and tax credit awards.

ICO established that employees were unaware of policies around disposing of confidential waste. In addition, the estate agent did not have a contract with data processors they used to securely dispose of data as required by DPA 7th Principle.

Undertakings:

1. By 31 December 2014 introduce formal and mandatory data protection training for all staff who handle personal data, to be repeated on a regular basis.
2. By 31 December 2014 review arrangements for storing confidential waste prior to collection by disposal companies and implement remedial measures.
3. Enter a written contract and keep a written record of companies used for secure disposal of personal data.
4. By 31 December 2014 review policies and procedures for compliance with the DPA.
5. Implement such other security measures as are appropriate to ensure personal data is protected.

Findings of ICO in relation to Undertakings signed:

1. N/A

Only ***51%*** of respondents to PwC's 2015 Information Security Survey said they had a security and awareness training programme. ***57%*** said they require employees to complete training on privacy policies.

(Source: PwC, *The Global State of Information Security Survey 2015*, 30 September 2014)

Treasury Solicitor's Department

27 August 2014

DPA – 7th Principle

Several breaches where personal data was disclosed in error to third parties. This included three incidents where case files were sent to a claimant's solicitor and then on to the claimant during the course of litigation.

Despite evidence that staff had been made aware of their obligations, ICO identified clear gaps in the measures to safeguard personal data.

Undertakings signed in February 2014:

1. Within 6 months implement a documented procedure for staff when preparing information for disclosure.
2. Within 6 months ensure the communication requirements between junior and senior lawyers making disclosures are clear and structured.
3. Within 6 months put in a place a mandatory compliance training programme for all staff.

Findings of ICO on 27 August 2014 in relation to Undertakings signed:

1. Documented procedure has been created for staff preparing information for disclosure.
2. It is now clear that senior staff sign off is required before disclosure is made.
3. The Treasury Solicitor's Department has taken appropriate steps to address the requirements of the undertaking, but further steps are needed:
   i. Data protection training should include content specific to information security and data protection policies, including a test element to ensure understanding.
   ii. Training material should be reviewed and updated periodically so it remains up to date with changes in the law and organisational policy.
   iii. Refresher training should be provided at appropriate intervals.

Racing Post

28 August 2014

DPA – 7th Principle

The Racing Post was subject to an internet based SQL injection attack. The hacker gained access to personal data affecting 677,335 data subjects which included: names, addresses, passwords, dates of birth and telephone numbers.

An investigation revealed that the attack was possible due to vulnerabilities in the website code. There had been no security updates on the website since 2007 which ICO viewed as an unacceptable risk to the security of personal data.

Undertakings:

1. By 28 February 2015 implement appropriate periodic security testing.
2. By 28 February 2015 implement a secure method of password storage in accordance with industry standards.
3. By 28 February 2015 define and implement an appropriate software update policy.
4. By 28 February 2015 compliance with internal data protection and IT security policies shall be monitored regularly.
5. By 28 February 2015 implement such other security measures as are deemed appropriate to ensure personal data is protected.

Findings of ICO in relation to Undertakings signed:

1. N/A

Total number of Undertakings

2014	2013	2012
29	22	31

Wirral Metropolitan Borough Council

29 August 2014

DPA – 7th Principle

Two separate incidents where two social work staff members sent information regarding two separate families to the wrong address resulting in the disclosure of sensitive personal data.

Whilst there was an ICT Security Policy in place, it did not contain suitable guidance in relation to data protection issues and it did not promote the use of locked printing. ICO was also concerned that before this incident data protection training was not mandatory.

Undertakings signed in April 2014:

1. Put processes in place to ensure documents are sent to the correct addresses and communicate guidance to staff.
2. Take steps to promote the use of locked printing functions or prompt collection of paperwork if locked printing is not used.
3. By 30 June 2014 ensure all staff complete mandatory data protection training.
4. Ensure mandatory data protection training for all staff is monitored and enforced in addition to updating training at regular intervals not exceeding 2 years.
5. By 30 June 2014 review data protection policies and procedures in order to comply with the DPA.
6. Implement such other security measures as are appropriate to ensure personal data is protected.

Findings of ICO on 29 August 2014 in relation to Undertakings signed:

1. Processes have been implemented to ensure documents are sent to correct addresses.
2. Secure/locked printing facilities are now in place where printers have this functionality.
3. Training completion is monitored.
4. New guidance documents have been created to ensure staff are aware how to comply with the DPA.
5. The council has taken appropriate steps to address the requirements of the undertaking, but further steps are needed:
   i. The council should replace printers that do not have locked printing functionality as soon as possible.
   ii. Policies and procedures to be reviewed regularly.
   iii. All staff who are yet to complete data protection training should do so as soon as possible.
   iv. Set a review date for training materials so they remain up to date with changes in the law and organisational policy.
   v. Staff should complete data protection training periodically.

Isle of Scilly Council

9 September 2014

DPA – 7th Principle

In June 2013 an attachment containing unredacted personal data was included in error within an email relating to an employee disciplinary hearing. The recipient was the employee subject to the disciplinary hearing and the union representative of the employee.

The Council had no formal data protection training in place at the time of the incident. ICO was also informed of another unauthorised disclosure of sensitive personal data via email occurring in September 2013.

Undertakings:

1. Implement and enforce mandatory data protection training concerning the use of personal data. Training should be recorded and monitored.
2. Set up a refresher programme to ensure data protection training is updated regularly.
3. Guidance should be communicated to staff when sending personal data by email, encryption of personal data should also be used where appropriate.
4. Implement a policy on the application of redactions.
5. Compliance with the council's data protection and IT security shall be regularly monitored.
6. Implement such other security measures as are deemed appropriate to ensure personal data is protected.

Findings of ICO in relation to Undertakings signed:

1. N/A

Oxford Health NHS Foundation Trust

22 September 2014

DPA – 7th Principle

In May 2013 whilst in the process of creating a new website, a 3rd party contractor unintentionally placed a file containing personal data on the internet relating to approximately 4200 users. The personal data included email addresses, usernames, passwords and billing addresses. Whilst human error was largely to blame, there was no data processor contract containing data protection provisions in place at the time of the incident.

There was also a second incident in January 2013 where a letter containing mental health information was sent to the wrong address. Human error was to blame once again, however on this occasion the Trust was unable to determine what steps had been taken to recover the letter to prevent further dissemination of its contents.

Undertakings:

1. Put in place adequate data processor contracts with all third parties processing personal data on the Trust's behalf, these should be in line with the NHS Information Governance Toolkit.
2. By 31 March 2015 introduce a procedure to conduct appropriate due diligence checks when selecting data processors.
3. By 31 March 2015 ensure appropriate information governance is in place and introduce PIAs for similar development projects.
4. By 31 March 2015 implement a breach management plan to cover appropriate containment and recovery obligations.
5. Implement such other security measures as are appropriate to ensure personal data is protected.

Findings of ICO in relation to Undertakings signed:

1. N/A

Norfolk Community Health & Care NHS Trust

25 September 2014

DPA – 1st, 3rd and 7th Principles

The Trust inadvertently shared data with a referral management centre. Files belonging to a third party had been shared in error, containing details relating to 128,842 data subjects consisting of information relating to referrals from health care services.

Although the data was transferred on an encrypted and password protected memory stick, there was a lack of instruction and communication to staff. In addition, whilst there was a contract with the referral management centre, there was no data sharing agreement or documented procedure for staff when compiling data sets. Both of these factors contributed to the incorrect sharing of the data.

Undertakings:

1. By 28 February 2015 implement and regularly review procedure for compiling and transferring data to third parties.
2. Ensure all staff are aware of data protection policies and procedures on an ongoing basis.
3. By 28 February 2015 ensure appropriate third party information sharing agreements are in place and a register maintained.
4. By 28 February 2015 contractual arrangements to contain safeguards on protection of personal data during and at the end of the contractual period.
5. Implement such other security measures as are deemed appropriate to ensure personal data is protected.

Findings of ICO in relation to Undertakings signed:

1. N/A

Increase in ICO enforcement actions due to cyber security incidents in 2014. In 2015 global IT security spending will increase by ***8.2%*** to ***$76.9 billion***

(Source: The Wall Street Journal, *Global Security Spending to Grow 7.9% in 2014, Gartner Says*, August 22, 2014)

Basildon and Thurrock University Hospitals NHS Foundation Trust

7 October 2014

DPA – 7th Principle

ICO was informed of two incidents where documents containing sensitive medical data were disclosed in error to third parties. The first incident, in July 2013, occurred when a letter was sent by a temporary staff worker to an incorrect recipient after two letters where accidently enclosed in the same envelope. The second incident, in October 2013, involved a doctor misplacing patient handover sheets when completing ward rounds, the sheets subsequently coming into the possession of a patient who should not have had access.

These were not isolated incidents, there have been several further instances where personal data has been incorrectly disclosed. ICO discovered temporary staff were not given the same level of training as permanent staff and the procedure for disposing of patient handover notes was routinely ignored.

Undertakings:

1. By March 2015, promote and monitor correct disposal of confidential information.
2. Permanent and staff workers to have consistent standards for handling personal data.
3. By March 2015, mandatory induction data protection training to be recorded and monitored.
4. By March 2015, consider implementing secondary peer review of documentation prior to posting.
5. Implement such other security measures as are deemed appropriate to ensure personal data is protected.

Weathersby Limited

8 October 2014

DPA – 7th Principle

An ftp server belonging to Weathersby was opened to external connections allowing anonymous access and had been indexed by Google. The server, which had been allowing anonymous access for 7 months, contained a moderate amount of personal data relating to 41 clients of Weathersby. The personal data included: identity documents, details of mortgage applications and two sets of bank account and payment card details.

Undertakings:

1. Mandatory information security awareness training to be introduced to all staff within 6 months of the undertaking.
2. Ensure all contractors working on the company's IT systems are given clear instructions about ensuring the security of the data controller's systems.
3. Implement such other security measures as are appropriate to ensure personal data is protected.

Findings of ICO in relation to Undertakings signed:

N/A

South Western Ambulance Service NHS Trust

8 October 2014

DPA – 1st, 3rd and 7th Principles

Seven discs containing detailed patient data relating to 45,431 data subjects were shared with a Clinical Commissioning Group (CCG) without a justifiable legal reason for doing so, as there was no sharing agreement in place.

ICO found that there was a lack of training with regards to staff training requirements with respect to data protection as sending the unencrypted discs by recorded delivery posed a security risk.

Undertakings:

1. Undertake a PIA in respect of any data sharing with CCG and any other organisation.
2. Ensure appropriate information sharing agreements are in place and maintain a register of agreements.
3. Amend notifications to ICO to cover form of processing as well as providing a privacy notice to reflect this exchange.
4. Ensure all staff undertake data protection training upon commencement of employment, this is to be recorded and monitored.
5. Set up refresher data protection training at regular intervals.
6. Implement such other security measures as are deemed appropriate to ensure personal data is protected.

Findings of ICO in relation to Undertakings signed:

1. N/A

Student Loans Company Limited

22 October 2014

DPA – 7th Principle

3 separate incidents where personal data was disseminated to incorrect recipients. Two of the incidents involved medical details containing sensitive personal data being disclosed to third parties in error, whilst the other incident involved 2 items of correspondence being sent to the wrong address.

ICO discovered that there were fewer checks in place when sensitive data was handled than when less sensitive data was handled, in order to reduce the number of individuals who could access sensitive personal data. It was also discovered that there had been several previous incidents of a similar nature.

Undertakings signed in April 2014:

1. Ensure appropriate procedures to guarantee that adequate checks are carried out on correspondences that contain sensitive personal data.
2. No later than September 2014 make the policy for storage and use of personal data, including the location and contents, available to all relevant staff.
3. Implement such other security measures as are appropriate to ensure personal data is protected.

Findings of ICO on 22 October 2014 in relation to Undertakings signed:

1. Review has been carried out to provide assurance on effectiveness of procedures for handling sensitive personal data.
2. Annual review for data protection policies and guidelines has been carried out.
3. Questionnaires and workshops have been created to make staff aware of DPA obligations.
4. Processes have been updated to include a DPA checklist to be updated each time sensitive personal data is sent externally.
5. DPA quality checks are being completed for an agreed period of time for staff who have been involved with an information security breach.
6. All DPA breaches, potential breaches, and failure to report are recorded.
7. 89% of staff have completed the data protection eLearning module by 15 July 2014.
8. In summary, ICO is satisfied that the Student Loans Company has taken appropriate remedial steps in response to the undertaking, but will continue to monitor issues of unauthorised disclosure.

The Royal Veterinary College

23 October 2014

DPA – 7th Principle

A memory card containing passport images of job applicants was stolen from a camera owned by a member of the Royal Veterinary College (RVC) staff. Although the memory stick was owned by the employee personally, RVC did not have a policy for employees using their own devices at work. ICO also considered that RVC's data protection training was not adequate.

Undertakings signed in October 2013:

1. By 30 April 2014, mandatory induction and refresher training to all staff who process personal data.
2. Training to be recorded and monitored at a senior level.
3. By 30 April 2014, all portable and mobile devices used to store and transmit personal data to be encrypted to meet current standards.
4. Implement physical security measures to prevent unauthorised access to personal data.
5. Implement such other security measures as are appropriate to ensure personal data is protected.

Findings of ICO on 23 October 2014 in relation to Undertakings signed:

1. All staff instructed to complete online data protection training by end of June 2014.
2. Process for monitoring and chasing those who have failed to attend training has been established.
3. Monthly reporting to RVC's CEO on data protection training statistics has been established.
4. Staff induction process now includes mandatory data protection training.
5. New laptops used for storing or transmitting personal data have been encrypted.
6. Door control systems have been installed which are centrally managed and recorded, and staff have also been given guidance on locking offices, computers and filing cabinets.
7. RVC's internal auditors have examined access controls to ensure security of personal data.
8. RVC has taken appropriate steps to address the requirements of the undertaking, but further steps are needed:
   i. 10 staff members have not received data protection training due to maternity or sick leave, this must be addressed.
   ii. Training material should be reviewed and updated periodically so it is up to date.
   iii. Refresher training should be provided at appropriate intervals to remind staff of data protection responsibilities.

Gwynedd Council

24 October 2014

DPA – 7th Principle

ICO was informed that a social care record relating to one individual was delivered to the wrong address. The error occurred due to the fact that the address was handwritten on the envelope making the house number unclear.

It was subsequently disclosed to ICO that there had been another breach whereby a social services file containing personal data relating to one service user had gone missing whilst being transported between two offices.

Undertakings:

1. Monitor and enforce mandatory data protection training, and provide refresher training.
2. Regularly remind staff of the policies for transportation, exchange and use of personal data and give appropriate training.
3. Implement such other security measures as are appropriate to ensure personal data is protected.

Findings of ICO in relation to Undertakings signed:

1. N/A

Disclosure & Barring Service

24 October 2014

DPA – 1st Principle

An undertaking was signed to amend question e55 of a Disclosure & Barring Service application form as it had not been amended since the relevant legislation came into force on 29 May 2013. It was also discovered that unamended application forms remain in circulation and this in ICO's view could result in unfair processing of personal data.

Undertakings:

1. As soon as practicable, but no later than 31 December 2014, legacy application forms containing the unamended question at e55 to be either rejected or removed from circulation.
2. Fortnightly updates to ICO as to progress in implementing this commitment.

Findings of ICO in relation to Undertakings signed:

1. N/A

London Borough of Barking & Dagenham

30 October 2014

DPA – 7th Principle

A letter containing a case file with medical data relating to 11 children was sent to an incorrect address. Although the information was not particularly detailed the file had still not been retrieved 5 months later.

ICO had previously given advice on improving its approach to containment and recovery in relation to personal data loss incidents, with a particular emphasis on speed of actions.

Undertakings signed in April 2014:

1. Ensure a procedure or policy is in place for when a loss of personal data occurs.
2. Ensure all staff are aware of this procedure or policy.
3. Ensure this policy contains specific and reasonable timeframes in which actions will be taken to retrieve personal data.
4. Implement such other security measures as are appropriate to ensure personal data is protected.

Findings of ICO on 30 October 2014 in relation to Undertakings signed:

1. The council has reviewed and revised policy for handling data breaches.
2. The policy has now been amended to include specific timeframes in which actions will be taken to retrieve personal data.
3. Action has been taken to make staff aware of the new policy.
4. The council has not yet fully complied with its undertaking commitments and should therefore take further action to:
   i. Ensure all staff complete the council's mandatory data protection training.
   ii. Carry out a data cleansing exercise to ensure staff training records are accurate and up to date.

46% of PwC clients have a mandatory process that requires the legal department to consider or review audit findings about security and data protection.

(Source: Legal Business, Anatomy of a breach, PwC Insight Report)

Department of Justice Northern Ireland

13 November 2014

DPA – 7th Principle

The Northern Ireland Prison service sold a filing cabinet at an auction in 2004 without removing files containing information relating to staff and inmates. A member of the public sent an email reporting the fact that he had found the documents.

Undertakings signed in May 2014:

1. Update record of condemned equipment to confirm that any assets used to store personal data have been securely emptied/ erased prior to removal.
2. By September 2014 all staff who handle personal data to receive induction and annual refresher training in requirements of the DPA.
3. All attendance at training is to be recorded and monitored.
4. Signed acknowledgments from staff showing they have read and understood information governance policies and procedures.
5. Implement such other security measures as are appropriate to protect against accidental personal data loss.

Findings of ICO on 13 November 2014 in relation to Undertakings signed:

1. Record of condemned equipment has been amended to confirm that personal data has been removed or wiped from condemned equipment.
2. Office relocation procedures have been updated and re-circulated to all staff.
3. Bespoke training has been provided to Senior Information Risk/ Information Asset Owners.
4. 'Responsible for Information' guidance booklets have been distributed to staff.
5. Staff are required to confirm acceptance of the Department of Justice's Security Operating Procedures before they can use IT systems.
6. However, despite the steps it has taken the Department of Justice Northern Ireland should take further action to:
   i. Ensure mandatory training is completed by all staff.
   ii. Ensure all training is logged and monitored.

Oxfordshire County Council

18 November 2014

DPA – 7th Principle

A solicitor dropped documents in the street relating to 3 child protection cases which contained sensitive personal data on 22 data subjects. The information included doctor's reports, mental and psychiatric reports and other medical professional correspondence.

The council could not prove that the employee had taken data protection training and it was discovered that there was no information on securing paper documents in its existing home working policy.

Undertakings signed in June 2014:

1. Put in place an adequate home working policy which includes guidance on security of paper documents.
2. Communicate availability of secure and lockable document transport cases.
3. Amend data protection policy to include specific guidance on removal of paper documents from the office environment.
4. Record and enforce completion of mandatory data protection induction training.
5. Implement such other security measures as are deemed appropriate to ensure personal data is protected.

Findings of ICO on 18 November 2014 in relation to Undertakings signed:

1. The council has put in place revised remote working policy including guidance on security of paper documents for staff working from home.
2. Remote working policy has been updated to include guidance on availability of secure lockable cases.
3. The data protection manual has been updated to include a section on paper records.
4. 100% of staff have completed mandatory data protection training.
5. Data breach reports have changed in both format and information gathered and will now be reviewed monthly.
6. However, despite the steps it has taken the council should take further action to:
   i. Implement changes to the HR system in order to monitor staff completion of data protection courses.
   ii. Ensure managers continue to communicate changes in Data Protection Manual and the Home Working Policy.

Aspers (Milton Keynes) Limited

25 November 2014

DPA – 7th Principle

An email containing personal data of 219 people was sent to an unauthorised third party. The personal data included bank details, dates of birth, national insurance numbers and home addresses.

The email was incorrectly sent to the third party in the process of attempting to communicate employee data to central payroll. The third party confirmed that they deleted the email.

Undertakings signed in June 2014:

1. Ensure an appropriate data protection and email policy is in place.
2. Make staff aware of policy for emails and use of personal data.
3. Ensure all employees who handle personal data receive regular data protection training.
4. Implement such other security measures as are appropriate to ensure personal data is protected.

Findings of ICO on 25 November 2014 in relation to Undertakings signed:

1. Data Protection Policy has been drafted and approved and communicated to staff in November 2014.
2. An IT policy covering acceptable use of email is disseminated to staff regularly.
3. Online data protection training has been developed and will be delivered to staff annually.
4. Information security risk assessment has been carried out of information systems and processes, mitigating actions have been identified.
5. The business intends to implement regular audits of the Data Protection Policy together with security testing of information systems and services.
6. In summary, Aspers has or is taking appropriate steps to address the undertaking requirements.

Dudley Metropolitan Borough Council

26 November 2014

DPA – 7th Principle

An agency social worker left a case file with sensitive personal data at a client's home. The documentation outlined a number of child welfare concerns raised by another family.

Undertakings signed in April 2014:

1. Ensure that members of staff use consistent standards in relation to handling personal data.
2. Ensure that mandatory induction data protection training is enforced for both permanent and agency staff and that training is monitored to ensure compliance.
3. Ensure guidance is available regarding taking personal information out of the office to social workers conducting home visits.
4. Implement such other security measures as are deemed appropriate to ensure personal data is protected.

Findings of ICO on 26 November 2014 in relation to Undertakings signed:

1. The review demonstrated that the council has taken some steps and put plans in place to address the requirements of the undertaking.
2. However, the council needs to complete further work to fully address all four requirements of the undertaking:
   i. Ensure agency staff declaration includes guidance as to taking information on home visits and out of the office.
   ii. Make sure all staff complete training and monitor training completion rates.
   iii. Migrate eLearning to a cloud based application.
   iv. Ensure all policies and high level guidance have named owners to set out clear ownership.

Caerphilly County Borough Council

19 December 2014

DPA – 1st Principle

The Council breached the DPA after it decided to undertake covert surveillance on an employee who was suspected of abusing the sickness in absence policy. The employee had been absent from work for four weeks for anxiety and stress when surveillance was authorised. Covert surveillance can be justified when there is suspected criminal activity or equivalent malpractice, but the ICO did not consider there to be sufficient evidence to warrant such action in this case.

Undertakings:

1. Follow the ICO Employment Practices Code when reviewing the employee surveillance policies and conducting future covert surveillance.
2. Follow, in particular, section 3 of the ICO Employment Practices Code covering the use of impact assessments.
3. Ensure that in every case an appropriate written impact assessment is completed.

Findings of ICO in relation to Undertakings signed:

1. N/A

International Trends

Belgium

New Secretary of State for Privacy

2014 has been a year of firsts in Belgium in privacy and data protection. In October 2014, in the shadow of the impending European legislative changes, Belgium appointed a State Secretary for Privacy for the first time. Together with the appointment of colleagues in charge of digital and cybercrime, the Belgian Federal Government has placed data protection and digital issues in a prominent position in the political agenda. This has not only raised awareness with both Belgian businesses and citizens, but has also created momentum to revisit lingering data protection issues surrounding social media, the Internet of things, drones etc. in addition to an increased application of the 'privacy by design' principle in various new initiatives.

Though it is too soon to tell how this change will impact the legislative and judicial branch of the Belgian state, there is already an increase in coordination, and even collaboration, between the Belgian State Secretary and the Privacy Commission on privacy issues affecting Belgium and Europe.

The Regulator

The Belgian Privacy Commission, officially named the "Commission for the Protection of Privacy" is the Belgian data protection authority and has been established as an independent commission under the auspices of the Belgian House of Representatives.

The Belgian data protection authority's main activities relate to the provision of information and assistance to national legislators and data protection stakeholders, enforcement, complaints and dispute resolution and, finally, supporting regulation and standardisation. The Privacy Commission regularly issues opinions, recommendations and other public communications on its website (www.privacycommission.be).

2013 report, published in 2014

The Commission reports on its activities in an annual report, and figures from the 2013 report published in 2014 show an overall increase in the number of interventions by the Commission. However, there was a fall in the number of data processing notifications filed by data controllers in Belgium (18%) compared to 2012. There was a notable increase in the number of complaints filed with the Commission (48.5%) mainly relating to privacy (27.6%), bad debtor registrations (13.6%), camera surveillance (12.4%), direct marketing (5.1%) and internet & social media (4%).

2014 report, to be published in 2015

The 2014 annual report is expected to be released towards the end of the spring 2015. We anticipate the next edition will highlight an increase in the number of interventions by the Privacy Commission, with employment related processing, cyber and camera surveillance as a continued area of focus (based on the recently launched landing page dedicated to the topic) . We also expect the number of complaints to rise, especially relating to the internet and social media, keeping in mind the growing level of awareness from businesses and individuals in addition to recent actions taken by the Belgian Privacy Commission and other EU data protection authorities against key social media players. Businesses are responding more actively to privacy concerns, particularly following data breaches (which have increased significantly in the past year) in no small part due to the direct impact these incidents have on their brand and reputation.

Court Cases

The Belgian Privacy Commission has always strived to reach amicable settlements, only turning to court proceedings in cases of severe or repeated breaches. However, the emphasis is now shifting, as the Commission is now openly considering court proceedings as a means of enforcement. The Belgian Privacy Commission has stated its intention to enforce more actively on the ground, with pilot projects already taking place in particularly sensitive sectors. The representatives of the Belgian Privacy Commission have been working more closely and sharing best practices with other data protection authorities.

We expect 2015 and beyond to contain increased activity from the Belgian data protection authority and the government. The emphasis will shift, from a "wait and see" approach, to a more active stance, taking action where needed for citizens and businesses, allowing Belgium to further develop its competitive advantage whilst preserving the rights and freedoms of all individuals. This will include more active enforcement and possibly an increase in litigation.

Carolyne Vande Vorst
+32 2 7109128
carolyne.vande.vorst@lawsquare.be

France

The French data protection agency (CNIL)

The CNIL supervises compliance with the law, by inspecting IT systems and applications. It also monitors the security of information systems by checking that all precautions are taken to prevent data from being distorted or disclosed to unauthorised parties.

Of particular note in 2014 is the CNIL's authorisation, under Article 44 Data Process Act (DPA), to carry out data privacy checks online without any prior notice to the data controller. Importantly, it is able to operate under a hidden identity. The findings of the CNIL's agents are recorded in minutes that are sent to the data controller, who in turn may respond with comments based on the CNIL's findings.

These online checks allow the CNIL to control:

- the relevance of the data collected (Article 6 DPA);
- the information notices to the public (Article 32);
- the security of data collected and processed (Article 34); and
- the reality of the indicated procedures (Articles 22 et Seq.).

Prosecutions and sanctions in 2014

There was a marked strengthening of the controls and increased level of fines in 2014. The key areas of focus were: the Register of Household Credit Repayment Incidents; the private data handling by electronic communication operators; online dating services; and the collection and storage of bank account information.

The CNIL can exercise the following sanctions:

- a fine (except in the case of government data processing) of a maximum amount of €150,000; and where similar previous offences have been committed, an amount of up to €300,000; or
- an injunction to stop processing and/or the withdrawal of the authorisation granted by the CNIL.

Financial sanctions

For the first time on 3 January 2014, the CNIL's Sanctions Committee ordered the maximum financial penalty sanction. This was issued to Google for infringing several provisions of the DPA and for not implementing enforced remedial actions within 90 days of the CNIL's formal notice. Google was ordered to pay €150,000.

Other financial sanctions include:

- 17 July 2014: €3,000 fine against the French Athletics Federation for a breach of duties concerning the publication of results on its website and of data confidentiality and privacy.
- 22 July 2014: €5,000 fine against Loc Car Dream for implementing a geolocation system that didn't comply with the DPA due to the excessiveness of the data that was processed.
- Public warnings and formal enforcements
- 28 April 2014 – a formal enforcement notice was issued against BNP Paribas Personal Finance, who were required within 2 months to erase information from the Register of Household Credit Repayment Incidents.
- 12 June 2014 – a public warning was issued against DHL for security breaches which affected the confidentiality of hundreds of thousands of client contact notices.
- 14 October 2014 – a formal enforcement notice was issued ordering Apple to comply with video monitoring regulations in Apple stores. Apple were required to move some in-store cameras and inform employees of video monitoring within 2 months.

Court Decisions

The French Court of First Instance of Caen, on 15 September 2014, ruled that a whistleblowing system designed for reporting misconduct relating to accounting and finance was illegal, because the reporting software available to employees did not clearly limit what could be reported under the system.

The French Cour de Cassation, on 8 October 2014, ruled that evidence collected on the basis of an automated personal data processing system prior to its notification to the CNIL was illegal.

The Criminal Court Judgment, on 18 December 2014, issued a €3,000 fine to an employee of Orange for creating a fake website about the deputy-mayor of Paris Rachida Dati by copying the photographs and graphic designs on his official site. This decision is the first regarding digital identity theft.

The outlook for 2015

In 2015, the CNIL has three major challenges to face: 1) the draft of the new EU data protection regulation, 2) developing co-operation between data protection authorities globally and 3) the conflict between the fight against terrorism and serious crime with the fundamental rights (protection of private life and private data) of all individuals.

The latter is demonstrated by a new drive from the French authorities to implement a French (or an EU) Personal Name Registration system to collect information on flight passengers in the wake of the despicable terrorist atrocities in Paris in January 2015.

Sophie Delahaie-Roth
+33 (0)3 90 40 26 10
sophie.delahaie-roth@fr.landwellglobal.com

Germany

Data protection in Germany is enforced and mandated by law in the private sector under the Federal Data Protection Act (Bundesdatenschutzgesetz) (BDSG), which implements Directive 95/46/EC on data protection. In general, the state data protection authorities' procedures are not made public unless they are matters of public interest. Once a year, however, they issue a report on their activities.

Privacy Incidents that became public through press in 2014:

Despite the fact that enforcement cases are rarely reported, below is an example of a case in 2014 where an organisation published a statement on its website regarding a fine for a privacy breach.

Health insurance firm fined €1,900,000 for privacy breach

In December 2014, as a penalty for ongoing privacy law violations, a health insurance firm settled on paying a fine of €1,900,000. The company was unlawfully acquiring addresses of potential customers that were later used by salesmen employed by the company to sell these people contracts.

Over a period of several years the insurance firm bought addresses of teachers and other public service employees to sell private health insurance contracts to them. The company claimed that these activities were only conducted by a few employees contrary to internal guidelines. Nonetheless, this incident was the reason for the state's data protection authority and the German Federal Financial Supervisory Authority ("BaFin") to act accordingly. The company cooperated during investigations and finally accepted the fine to avoid trial.

Sentence:

The fine was split as a €1,300,000 penalty and an additional €600,000 to establish a university institute to support research on data protection and privacy. Following this case the BaFin published guidelines on ad hoc advisors.

Jan-Peter Ohrtmann
+49 (0) 211 981 2572
Jan-peter.ohrtmann@de.pwc.com

Tobias Gräber
+49 (0) 211 981 1837
tobias.graeber@de.pwc.com

Italy

This is a short summary of the enforcement action taken by the Italian Data Protection Authority (IDPA) in 2014.

In June each year the IDPA issues its Annual Report containing a summary of the activities and decisions in the previous year. June 2015 will be an important milestone to analyse the enforcement trends in 2014.

Nevertheless, an analysis of the June 2014 report reveals key areas of focus for the IDPA. The decisions were focused on: marketing activity via telephone; video surveillance in the workplace and remote control over employees; data protection on social networks; transfer of data to foreign countries; and utilization of "traffic data" processed by providers of public communications networks.

Telecomunications data

The most significant financial penalty in 2014 (€300,000) was issued against a data controller that collected personal data from the unique database of telecommunications providers and made the data available to third parties through its website. The main reasons for the level of the sanction were: the processing of data for marketing purposes without providing a privacy statement and obtaining consent of the data subjects; the failure to comply with previous decisions made by the IDPA; and failure to provide the IDPA with the documentation and information requested.

Direct marketing

The second highest sanction of 2014 (€112,000) was issued against a company that contacted 4 data subjects for marketing purposes, all of whom had exercised their opt-out right by registering their phone numbers in the Public Register of Oppositions. The penalty was issued for: the failure to provide the privacy statement (€12,000), the failure to obtain the prior consent for marketing purposes (€20,000) and contacting data subjects who had exercised their opposition right (€20,000 for each).

Several other cases have been pursued by the IDPA for illicit phone calls for marketing purposes. In 2 cases the IDPA issued sanctions of €40,000 for phone calls made by concealing the identity of the data controller. In the first case, the amount was calculated as €20,000 for each phone call. In the second case the IDPA issued a €20,000 fine for the concealing identity and €20,000 for the failure to obtain the consent of the data subject.

The IDPA takes into account certain important features when determining the size of a fine. The IDPA considers the level of cooperation of the data controller during proceedings; the activities to mitigate the effect of any breach of the law and the financial power of the data controller.

Video surveilance

In 2014 the IDPA issued significant sanctions (€40,000) for the use of video-surveillance systems when the data controller did not: (i) provide the necessary privacy statement; (ii) adopt the security measures for processing of data with electronic means and (iii) follow the instructions given by the IDPA on video surveillance (including the appointment of a person responsible for data processing and the time limits for the registration of the data).

Right to be forgotten

In 2014, the IDPA also addressed the "right to be forgotten" following the Google Spain case - a judgment which is likely to have significant ramifications for European data privacy law in 2015. There were 9 instances in Italy in 2014 where the IDPA ruled that Google must remove information about the data subjects from Google search engine results. However, 7 claims were rejected as the IDPA ruled that there was a clear public interest in accessing the information. Google Spain type cases is a trend that we can expect to intensify in 2015.

Stefano Cancarini
+39 0291605212
Stefano.Cancarini@it.pwc.com

Lithuania

A number of high profile data security breaches in both the public and private sectors over the last few years have put data security issues to the fore in the Lithuania. Individuals are becoming more vocal when it comes to the protection of their privacy and personal data, which is evidenced by an increasing number of data access requests and complaints submitted to the Lithuanian data protection authority – the State Data Protection Inspectorate (SDPI). In recent years the SDPI has made an increased effort to force Lithuanian companies to fully understand and become truly responsive to new confidentiality and data protection challenges.

Direct marketing

In 2014 the SDPI received numerous complaints concerning direct phone marketing from people who had not given their prior consent. Marketing companies tried to argue that the phone number generated randomly does not relate to a specific person and hence cannot be considered personal data. The courts have ruled several times (e.g. Vilnius Country Court decision of 14 February 2014 in case A2.11.-1793-295/) that it is possible to identify a person from a phone number (i.e. by asking for a person to confirm their name when that person picks up the phone). Consequently, as the phone number held by an individual is for private use, it is deemed to be a part of an individual's personal data. The violation of direct marketing regulations is a fairly frequent occurrence in Lithuania.

Despite this, personal data protection is not treated as a very sensitive issue in Lithuania. The maximum fine for violation of personal data protection rules is a derisory €580 and only applies to the management of an organisation. One of the main problems is that there is a lack of understanding among local companies that by breaching personal data protection regulations they can face serious reputational consequences.

Pharmaceutical

Reputational risk is clearly an important issue for companies acting in more regulated sectors of the economy e.g. pharmaceuticals. For ethical reasons, pharmaceutical companies operating in Lithuania have recently agreed to start disclosing to the public very detailed information about money (e.g. donations and other benefits) transferred to healthcare institutions and healthcare specialists. This agreement has created a data protection problem. It is necessary to obtain very detailed consents from each healthcare specialist because companies will have to administer and secure large amounts of personal data. Most pharmaceutical companies have introduced extended procedures required for the management of such personal data, and have opened a dialogue with the SDPI.

Cyber security

Another issue that may urge local companies to undertake greater commitments to data security systems is cyber security. Key factors such as the Snowden affair and politically driven discussions in the US and EU on global data protection, have caught the attention of the Lithuanian public. At the end of 2014, Lithuania passed the Law on Cyber Security to enhance the protection of the country's cyber space. The legislation ensures that there are necessary resources to thwart attacks and keep cyber space safe for all users. Because most of the IT infrastructure is managed by private companies, the private companies are also required to guarantee cyber security of personal data. In particular, providers of communications (including providers of access to internal networks or cloud storage facilities) are required to report to authorities about cyber security violations (e.g. unauthorised access to their networks, leakage of internal data or other related violations of network integrity) and inform users about the steps being taken to safeguard cyber security. The Law on Cyber Security established the National Cyber-Security Centre which coordinates cyber-defence issues. It requires businesses to take a closer look at the flaws in their security systems and start rectifying the vulnerabilities in their data protection policies.

In conclusion, although data protection is attracting a greater awareness from the general public, until the relevant EU laws (the proposed Data Protection Regulation) are adopted, data protection will remain an important but unresolved problem for domestic and international businesses operating in Lithuania.

Rokas Bukauskas
+ 370 (5) 239 2341
rokas.bukauskas@lt.pwc.com

Evelina Agota Vitkutė
+ 370 (5) 239 2324
evelina.vitkute@lt.pwc.com

Mexico

The Federal Institute for Access to Information and Data Protection (IFAI), is the Mexican data protection authority in charge of promoting awareness on personal data protection, promoting its exercise, and overseeing the due observance of the provisions issued; in this sense, the IFAI publishes its resolutions regarding data protection processes due to its transparency obligations derived from the observance of the Federal Law of Transparency and Access to Public Government Information. However, it should be acknowledged that there is still a long way to go to promote data protection as a critical political and regulatory issue in Mexico. This section will provide a short overview of the legal framework.

Data Protection acquired relevance in 2009, when a Constitutional Reform to Article 16 was published in the Federal Official Gazette, stating: "Every person is entitled to protect, access rectify, cancel or object to the processing of his personal data, within the terms established by the law, which provides the exemptions to the principles regarding national security, domestic public policy provisions, public health and safety or to protect third parties' rights." This reform appointed the IFAI as the Mexican Data Protection Authority

Following this, the Federal Law on the Protection of Personal Data held by Private Parties (Law), entered into force in July 2010. The Law concerned protecting personal data held by private parties, in order to regulate its legitimate and controlled processing, to ensure the privacy and rights of individuals. The integration of the legal framework was followed with the Regulation, which entered into forced in December 2011.

The IFAI has the power to issue fines from 100 to 320,000 days of the General Current Minimum Wage in Mexico. Where a breach includes processing sensitive personal data, the sanctions may be doubled.

The IFAI will base its decisions on the following factors:

- The nature of the personal data concerned;
- The refusal of the data controller to perform the actions requested by the data subject;
- The intentional or unintentional nature of the action or omission constituting the infringement;
- The financial capacity of the data controller; and
- Repeat offences.

There is also the possibility of the following criminal sanctions if there is unlawful processing of personal data (sanctions are doubled where sensitive personal data is involved):

- **Three months to three years imprisonment** - any person who is authorized to process personal data, for profit, who causes a security breach affecting the databases under his custody.
- **Six months to five years imprisonment** - any person who, with the aim of achieving unlawful profit, processes personal data deceitfully, taking advantage of an error of the data subject or the person authorized to transmit such data.

Financial Sanctions

- c. $90,200 fine against Real Estate Sellers for improper use of personal data on a public advertisement. The data subject's personal and family information was used without consent.
- c. $44,300 fine against ASLA 21, trading name Pronto Prestamo, for ignoring a subject access and data cancellation request.
- c. $8,500 fine against Creaciones Textiles de Mérida for their lack of a privacy policy, meaning a data subject could not exercise his 'ARCO' rights (Rights of Access, Rectification, Cancellation and Objection).

Wendolin Sánchez
+52 (55) 5263 8578
wendolin.sanchez@mx.pwc.com

Poland

In 2014 the Polish personal data protection authority (General Inspector for Personal Data Protection, GIODO) received nearly 2,500 complaints from data subjects on how their personal data was being processed. This marks a steady increase over a number of years in the amount of complaints the GIODO received, in 2013 there were 1,900 complaints and in 2012 there were approximately 1,600.

In 2014 the GIODO made approximately 1,200 decisions, 500 of which were related to data filing system registrations.

Churches

There was a common trend in 2014 (often in Catholic churches) that church goers became aware that their personal data was being processed by church authorities in church books. Church authorities refused to delete the data either due to procedural issues or as a result of an interpretation that such data should remain unchanged as they are important historical records.

The GIODO had to decide whether such a situation was within its jurisdiction (a critical point, as relations between churches and Polish authorities are regulated in special acts) and whether the request from those who demanded that their data should be deleted or corrected should be enforced. In some decisions (e.g. decision dated 16 September 2014, DOLiS/DEC-908/14/72365,72366) the GIODO enforced the right to the correction of the data, whereas in other cases (e.g. decision dated 14 April 2014, DOLiS/DEC-374/14/29069,29070) the GIODO decided to end proceedings without any enforcement due to the fact that the church authorities were no longer processing the data.

Internet users

People who victimise others on the Internet are often able to remain anonymous, yet victims often want to find the perpetrator's personal information to enforce their rights in legal proceedings. In Poland this kind of personal data is protected under the law on personal data protection, but there is a question of whether a website owner may reveal the infringer's personal data to the victim.

This was an issue that the GIODO had to respond to countless times during 2014. In its decisions the GIODO either enforced the right to reveal the personal information (e.g. decision dated 19 December 2014, DOLiS/DEC-1202/14/100586,100592) or refused – however, the latter was mostly due to the applicant not following the correct procedures (e.g. decision dated 7 May 2014, DOLiS/DEC- 429/14/34658,34672).

Other decisions

Other decisions of the GIODO related to marketing activities of data controllers (mostly unsolicited telephone calls or mailing); data controllers not fulfilling information obligations towards data subjects; lack of entrusting personal data processing to data processors; and improper methods of obtaining consent for personal data processing.

Financial penalties

Under Polish law, the GIODO is not authorised to issue financial penalties in cases of personal data protection law breaches. However, if the GIODO makes a decision on a breach and the organisation or individual at fault does not act in accordance with the GIODO's instructions, then they may impose a financial penalty to enforce the decision. However, examples of this are rare. By way of example, in 2013 the GIODO only imposed two such financial penalties - each amounting to just €6,000 each.

Anna Kobylańska
+48 (0) 519 50 6226
anna.kobylanska@pl.pwc.com

Russia

2014 witnessed several key developments in data privacy and security in Russia, below is a high level overview of some of the key developments and trends.

Online privacy

Privacy and security enforcement on the part of the Russian data protection authority, the Federal Supervision Agency for Information Technologies and Communications (Roskomnadzor) continued to evolve. Roskomnadzor actively pursued websites that illegally make the personal data of Russian citizens available. In July 2014, Roskomnadzor blocked the website telkniga.com, which featured the personal data of Russian citizens. The legal premise behind this action was a decision of the Angaskiy District Court in the Irkutsk Region on a lawsuit brought by Roskomnadzor in the interest of the general public due to the unlawful processing of personal data. Previously, the Butyrskiy District Court of Moscow issued a similar decision with regards to the websites Naidiludey.com, Stockphone.org, and Bazaludey.com.

Since 2014, Roskomnadzor has filed 28 lawsuits in order to block 96 Internet resources, which have been accused of unlawful dissemination of personal data. Currently, nine court decisions on the blocking of sixteen Internet resources are in place, while another nineteen cases are going through the court system at the moment.

Social media

One major development in 2014 was Roskomnadzor's demand that foreign online social media services like Twitter, Google and Facebook must meet the requirements of the Russian law on the blocking and disclosure of certain information. These companies have received respective requests from the regulator to comply with Russian law.

ISPs

Since 2014 it has been an obligation for internet service providers (including message boards, social networks, indexing, email services, etc.) to store certain data on their users' Internet activities in the Russian Federation for a period of six months. Russian law enforcement agencies may request such information from companies. However, at the moment, no enforcement practice is in place to enforce this rule.

New storgage law

Looking forward to later this year, effective from 1 September 2015, the personal data of Russian citizens must be stored, processed and maintained in databases located in Russia. Roskomnadzor has been given the legal authority following a court decision, to limit access to personal data that has been processed in violation of this rule (e.g. blocking of website domain names, network addresses, indexes of pages, etc.).

Evgeniy Gouk
+7 (812) 326-6969
evgeniy.gouk@ru.pwc.com

Spain

The major trends set out below show that the Spanish Data Protection Authority (SDPA) and the Spanish court system made an increased effort in 2014 to protect personal data and ensure that it is a topic at the forefront of the political and social agenda.

The following developments send a clear message to businesses in Spain to review their policies and the policies of their business partners, to ensure compliance and good practice with respect to the collection, retention, processing and transfer of personal data.

Spanish National High Court and "the right to be forgotten"

The Spanish National High Court made the first judgments based on the criteria set by the Court of Justice of the European Union (ECJ) in their judgment in Case-131/12 (Google Spain SL, Google Inc. v Agencia Española de Protección de Datos) on 13 May 2014. The judgment referred to both appeals brought by Google Spain and Google Inc. against the requirement of the SDPA for Google to remove the claimant's personal information from their index and search results.

Content of the judgment

Google's activity, consisting of finding and indexing personal information, constituted processing of personal data. Google, as a data controller, was compelled to take appropriate measures to remove personal data in accordance with Spanish data protection legislation.

The High Court determined that the prevalence of the claimant's rights (namely, the opposition right) were not absolute and the claimant's personal circumstances must be taken into account. Interference or limits to a claimant's rights may only be justified when it is necessary to protect the interests of a democratic society.

In this particular case, the claimant appeared on a list of results in a Google web search which linked to La Vanguardia's website in January and March 1998. The information related to a real-estate auction following proceedings for the recovery of social security debts the claimant owed. Google was required to remove the information from search engine results.

First cookies disciplinary resolutions

In 2014, the SDPA issued its first disciplinary resolutions regarding cookies.

Google was among the companies fined by the SDPA. They were fined €25,000 for breaching article 22.2 of the Spanish Law on Information Society Services and Electronic Commerce. The SDPA found that Google did not inform customers using its "Blogger" service on how cookies were used and the specific purposes for which personal data was processed.

The SDPA has also issued various legal reports and resolutions on cookies, based on the principles set out by the Article 29 working party, aimed at clarifying the information to be provided in the second information layer. The SDPA considers it permissible to show additional information on a second layer when:

i. cookies have the same identity or nature; and

ii. the information is not ambiguous.

Data Protection Impact Assessment Guide

The SDPA released the Data Protection Impact Assessment Guide (DPIA) in October 2014. The key points are as follows:

a. Although the DPIA is not currently legally binding in Spain, it aims to promote data protection good practice by providing a flexible framework which goes further than mere 'compliance'.

b. The DPIA is specifically directed at organisations who process vast amounts of personal data. It provides examples of scenarios where it would be advisable to perform an impact assessment analysis by identifying potential risks and implementing remedial measures.

c. It is evident that Spanish organisations that follow the DPIA methodology will be one step ahead when the General Data Protection Regulation enters into force.

System for the notification of personal data breaches

In April 2014, following the European Commission Regulation 611/2013, the SDPA launched an online reporting system designed to make it easier for "providers of publicly available electronic communications services" to notify the regulator in the event of personal data security breaches.

Carlos Rodríguez Sau
+34 619 077 612
carlos.rodriguez.sau@es.pwc.com

Ruben Cabezas Vázquez
+34 638 343 340
ruben.cabezas.vazquez@es.pwc.com

Sweden

Overview

In Sweden, the Data Inspection Board (DIB) has the responsibility to enforce the Data Protection Act, the Debt Recovery Act and the Credit Information Act. They have a mandate to focus on sensitive areas, new trends and areas with an increased risk of privacy violations. They perform inspections in two ways: by visiting an organisation for inspection or by sending out a survey. The DIB has the power to issue penalties - although in 2014 no fines were issued. The DIB will often provide advice on how an organisation can improve its privacy policies and procedures and/or make them sign undertakings. Any decision or penalty issued by the DIB may be appealed in the Administrative Court.

An inspection may be made by the DIB acting of its own accord, based on a complaint from a data subject or on a notification from a Personal Data Representative (PDR). A PDR is obliged to notify the DIB if the organisation does not implement the PDR's request to rectify identified violations of the Personal Data Act. The PDR role is similar to the DPO role, but there are no formal competency requirements. It is voluntary for an organisation to appoint someone, and if they do, then they do not need to notify the Data Inspection Board that they process personal data. The PDR is expected to ensure that an organisation complies with the Data Protection Act by providing appropriate related advice.

Enforcement actions

Below is a high level overview of the actions of the DIB in 2014:

- Camera surveillance: 5 (2 manufacturing companies, school, hotel, shop).
- Credit Information: 8 (credit Information companies only).
- Debt Recovery: 41 (debt recovery companies and electric power suppliers).
- Personal Data: 157 (health care, research, customs, police, real-estate companies, telecom and internet providers, internet service providers, energy companies, non-profit organisations, social welfare, insurance companies, authorities, railway, public authorities, courts, restaurant, banks).

Prosecutions and appeals (2014 examples)

July 2014: Salem's Municipality appealed against a decision made by the DIB that they were not allowed to use Google cloud service apps, as the agreement with Google did not comply with the requirements in the Data Protection Act. The Administrative Court rejected the appeal.

November 2014: A Norwegian employment agency, Accurate Care AS, appealed against the National Board of Health and Welfare's decision, based on "Public access to information and secrecy act", not to provide requested information about identification cards issued to Swedish nurses. Accurate Care intended to use the information in their recruitment activities. The Supreme Administrative Court decided that the company should get the information, since the Swedish Data Protection Act is not valid in Norway. This lead to a prominent debate in the media about the legal loophole this case revealed.

Electronic communications

The Swedish Post and Telecom Authority (PTS), has the responsibility to enforce data protection and privacy requirements in the Swedish Electronic Communication Act and the Data Breach Notification Regulation. The PTS has issued guidance on how to report data breaches and provides a reporting system to be used by the operators in Sweden. Generally speaking, the number of data breaches reported to the PTS is very low.

In 2014 there has been a vociferous debate in the media regarding telecom operators' data retention obligations. The telecom operators in Sweden ended up in an unclear situation regarding the data retention requirements in the Electronic Communications Act, since it was decided in March that the EU directive on which it was based was invalid. Tele 2 and several other telecom operators decided not to retain traffic data. The Administrative Court decided in October that the operators still have to provide traffic data in accordance with instructions from PTS, despite the decision invalidating the EU directive.

Göran Laxén
+46 (0) 709 29 19 29
goran.laxen@se.pwc.com

Switzerland

In Switzerland, The Federal Data Protection Commissioner does not yet have the resources and authority to investigate data privacy violations, and the potential level of fines provides little deterrent - Data Protection is not a topic at the top of the compliance agenda. That is why Data Privacy cases in Switzerland are much less common than in other comparable European jurisdictions e.g. the UK.

Here is an overview of important activities of the Federal Data Protection and Information Commissioner (FDPIC) in 2014.

Workplace issues (Swiss Banks, Spring 2014)

After making a number of recommendations to five banks in 2012 on the subject of tax disputes with the USA, and in order to find an acceptable solution to this on-going problem, the FDPIC published an information guidance sheet which regulates how banks who wish to transfer personal data to the US tax authorities should go about doing so.

Currently, various lawsuits in connection with personal data transfers from Swiss Banks to US tax authorities are pending judgment in the Swiss court system. In many cases the action required was a temporary transfer block, but no final judgment was delivered in 2014.

PostFinance, Switzerland (October 2014)

Customers of PostFinance, a Swiss Bank, were asked to agree to new terms and conditions to accept participation in the new Bargain-Service-Portal, if they wanted to continue to use PostFinance's e-banking system. PostFinance planned to make use of the digital footprints left behind by PostFinance customers when paying with a credit card or making payments via online banking. PostFinance intended to scrutinise the profiles and behaviours of customers so that they could tailor rebate programs from third parties on each customer individually. In October 2014 the FDPIC intervened. In dialogue with the company, the FDPIC concluded that customers have a right to object (opt-out), explicitly prohibiting analysis of their personal data for marketing purposes, therefore avoiding offers from third parties.

Business and commerce

This year, the FDPIC carried out a number of follow-up checks on customer cards issued by the two largest Swiss retailers. The evaluation process is still ongoing and the findings are yet to be confirmed.

Recommendations were made to Moneyhouse, a Swiss commercial register database, that it should modify its address recording system. The FDPIC monitored the implementation of the recommendations, which proved to be a time-consuming exercise. There have been several complaints since the operator of the service, Itonex AG, modified the deletion protocols. The FDPIC has provided advice to the individuals concerned and is in the process of analysing the services offered by Itonex AG - the outcome of this analysis is expected later this year.

Credit rating databases

Finally, an important trend in 2014 is that owners of credit rating databases must ensure that they take into consideration security needs when handling requests for the deletion of data. However, it is important for individuals making such requests to bear in mind that having their data deleted from these databases could have adverse consequences on their businesses.

Susanne Hofmann
+41 (0)58 792 1712
Susanne.hofmann@ch.pwc.com

USA

Privacy Enforcement Actions in the U.S. Set All-Time Record

Regulators and courts imposed more than $900 million in fines and penalties in 2014 for data privacy and security shortcomings, shattering the 2013 tally of $74 million for all jurisdictions and regulators worldwide.

Federal Trade Commission (more than $341,430,000 in penalties)[i]

The Federal Trade Commission (FTC), which enforces an array of consumer-facing privacy laws and regulations, concluded its most prolific year on record with regard to privacy-related settlements:

- Federal appeals court upheld district court ruling that imposed more than $163 million on a defendant for her role in persuading consumers into thinking their computers were infected with malicious software, and sold them software to "fix" their non-existent problem.
- Settled allegations that a marketing company tricked consumers into buying phone health insurance through deceptive telemarketing. The settlement bans the company from selling healthcare-related products and includes a $125 million judgment.
- Action jointly brought with the Florida Attorney General against an information services company resulted in a $23 million settlement to permanently stop an operation used to pre-record telephone calls, or "robocalls".
- Settled charges for $10 million with defendants for sending unwanted text messages to consumers and for potentially violating the FTC Act and the TSR.
- Fined a collection of companies that were posing as major computer security and manufacturing companies $5.1 million in redress for deceiving consumers into believing that their computers were riddled with viruses, spyware, and other malware. The companies were not actually affiliated with major computer security or manufacturing companies, but charged consumers hundreds of dollars to access and "fix" the consumers' computers.
- Settled charges for $4.2 million that affiliate-marketing companies sent millions of spam texts to consumers.
- A check authorization-service company agreed to pay $3.5 million to settle claims it violated the FCRA.
- Settled with a holding company that was sending millions of spam messages to consumers falsely promising "free" gift cards. The company agreed to pay $2,863,000.
- Settled with 12 website operators that enticed consumers with bogus offers and hired affiliates to send spam text messages to promote them. The defendants agreed to pay $2.5 million.
- Settled with a data broker for allegedly violating the FCRA by failing to provider adverse action notices to consumers. The company and its owners agreed to pay $1 million.
- Settled with a data broker for allegedly violating the FCRA and providing reports about consumers to users, such as perspective employers. The case imposed a $525,000 fine.
- Settled charges with a restaurant app for collecting personal information from children without first notifying parents. The company agreed to pay a $450,000 civil penalty.
- Filed a complaint against a gaming company's popular apps for allegedly failing to follow COPPA-required steps. The company agreed to pay a $300,000 civil penalty.

Federal Communications Commission ($112,400,000 in penalties)

The Federal Communications Commission (FCC), which enforces telephone privacy-related laws and regulations, entered the privacy-enforcement arena with a bang:

- Settled with a mobile-phone service provider for $105 million to resolve an investigation into allegations that the company billed customers millions of dollars in unauthorized third-party subscriptions and premium text messaging services; this is the largest settlement in FCC history.[ii]
- A leading mobile-phone service provider agreed to a $7.4 million settlement with the FCC to resolve an investigation into the company's use of personal consumer information.[iii]

U.S. Department of Health and Human Services ($6,225,000 in penalties)

The U.S. Department of Health and Human Services, principally through its Office of Civil Rights, also stepped up its pace of enforcement actions in 2014:[iv]

- A hospital agreed to pay $3,300,000 to settle HIPAA violations related to data breaches as well as adopt a corrective-action plan to evidence their remediation findings.
- A health-services organization paid a $1,725,220 settlement for potential HIPAA violations related to stolen laptops.

i. Federal Trade Commission 2014 Privacy and Data Security Update; https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2014/privacydatasecurityupdate_2014.pdf

ii. Federal Communications Commission Consent Decree; http://www.fcc.gov/document/att-pay-105-million-resolve-wireless-cramming-investigation-0

iii. Federal Communications Commission Consent Decree; http://www.fcc.gov/document/verizon-pay-74m-settle-privacy-investigation-0

iv. HHS.gov Case Examples and Resolution Agreements; http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/

v. Hospital Agrees to Pay $190 Million Over Recording of Pelvic Exams; http://www.nytimes.com/2014/07/22/us/johns-hopkins-settlement-190-million.html?_r=0

- A university agreed to settle potential HIPAA violations with a $1,500,000 monetary settlement as well as implement a corrective-action plan to address deficiencies in its HIPAA compliance program as a result of a data breach.
- A health system paid a $800,000 settlement for a potential HIPAA violation as well as agreed to adopt a corrective-action plan to correct deficiencies in its compliance program.
- A health plan agreed to settle potential HIPAA violations related to stolen laptops for $250,000 settlement to correct deficiencies in its compliance program.
- A county government settled a $215,000 claim for potential HIPAA violations.
- A mental-health service organization settled potential HIPAA violations for underscoring the vulnerability of unpatched and unsupported software. The organization paid $150,000 and adopted a corrective-action to correct noted deficiencies in its HIPAA compliance program.

Class-action lawsuits resulting in damages ($190,000,000 in penalties)

U.S. courts also produced the largest class-action settlement on record related to privacy violation claim:[v]

- A hospital agreed to pay $190 million to thousands of women in a class-action lawsuit for a doctor's direct violation of doctor-patient trust. The civil suit charged the hospital with invasion of privacy, emotional distress, and negligence of its oversight of the doctor in question.

Jay Cline
+1 763 498 2237
jay.cline@us.pwc.com

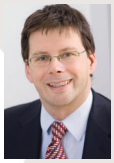
Team and contact information

UK Lawyers

Stewart Room
Partner
+44 (0)20 7213 4306
stewart.room@pwclegal.co.uk

Latika Sharma
Partner
+44 (0)20 7212 1574
latika.sharma@pwclegal.co.uk

Michael Gorrill
Head of Data Protection Enforcement and Regulatory Affairs
+44 (0)161 245 2546
michael.gorrill@pwclegal.co.uk



Jonathan Nugent
Senior Manager
+44 (0)20 7804 2060
jonathan.nugent@pwclegal.co.uk

Krysia Sturgeon
Senior Associate
+44 (0)20 7212 5504
krysia.sturgeon@pwclegal.co.uk

Tughan Thuraisingam
Trainee Solicitor
+44 (0)20 7804 3770
tughan.thuraisingam@pwclegal.co.uk

Oliver Pike
Trainee Solicitor
+44 (0)20 7804 2637
oliver.t.pike@pwclegal.co.uk

John McGonagle
Manager
+44 (0)20 7213 8303
john.d.mcgonagle@pwclegal.co.uk

Nigel Wilson
Senior Manager
+44 (0)20 7213 1655
n.wilson@pwclegal.co.uk

James Witton
Trainee Solicitor
+44 (0) 207 804 2509
james.witton@pwclegal.co.uk

UK Risk Assurance, Consulting, Cyber Security and Forensics

Kris McConkey
+44 (0)20 7804 2471
kris.mcconkey@uk.pwc.com

Richard Horne
+44 777 555 3373
richard.horne@uk.pwc.com

Jane Wainwright
+44 (0)20 7583 5000
jane.a.wainwright@uk.pwc.com

Gavin Siggers
+44 (0)20 7804 4026
gavin.d.siggers@uk.pwc.com

Mark Hendry
+44 (0)1895 52 2066
mark.hendry@uk.pwc.com

Jessica Tay
+44 (0)20 7804 7592
jessica.tay@uk.pwc.com

Radhika Bogahapitiya
+44 (0)23 8083 5035
radhika.p.bogahapitiya@uk.pwc.com

Rahul Colaco
+44 (0)20 7213 2663
rahul.p.colaco@uk.pwc.com

PwC Legal does not provide legal services in the USA, nor do we provide advice or opinions on matters of US law

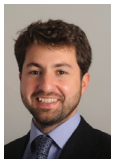
International Lawyers

Jan-Peter Ohrtmann (Germany)
+49 211 981-2572
Jan-peter.ohrtmann@de.pwc.com

Tobias Gräber (Germany)
+49 (0) 211 981 1837
tobias.graeber@de.pwc.com

Anna Kobylanska (Poland)
+48 (0) 519 50 6226
anna.kobylanska@pl.pwc.com

Carlos Rodriguez Sau (Spain)
+34 915 684 325
carlos.rodriguez.sau@es.pwc.com



Ruben Cabezas Vasquez (Spain)
+ (34) 915 684 400
Ruben.cabezas.vazquez@es.pwc.com

Assumpta Zorraquino Rico (Spain)
+34 932 532 507
assumpta.zorraquino@es.pwc.com

Carolyne Vande Vorst (Belgium)
+32 2 7109128
carolyne.vande.vorst@lawsquare.be

Stefano Cancarini (Italy)
+39 02 91605212
stefano.cancarini@it.pwc.com

Paola Barazzetta (Italy)
+39 02 916051
Paola.barazzetta@it.pwc.com

Andrey Odabashian (Russia)
+7 (812) 326-6969 ext. 4560
andrey.odabashian@ru.pwc.com

Evgeniy Gouk (Russia)
+7 (812) 326-6969
Evgeniy.gouk@ru.pwc.com

Rokas Bukauskas (Lithuania)
+ 370 (5) 239 2341
rokas.bukauskas@lt.pwc.com

Evelina Agota Vitkutė (Lithuania)
+ 370 (5) 239 2324
evelina.vitkute@lt.pwc.com

Yvette van Gemerden (Netherlands)
+31 88 792 5442
yvette.van.gemerden@nl.pwc.com

Folkert Hendrikse (Netherlands)
+31 (0) 887924972
folkert.hendrikse@nl.pwc.com

Susanne Hofmann (Switzerland)
+41 (0)58 792 1712
Susanne.hofmann@ch.pwc.com

Sophie Delahaie-Roth (France)
+33 (0)3 90 40 26 10
Sophie.delahaie-roth@
fr.landwellglobal.com

Wendolin Sánchez (Mexico)
+52 (55) 8263 8578
wendolin.sanchez@mx.pwc.com

Tony O'Malley (Australia)
+61 (2) 8266 3015
tony.omalley@au.pwc.com

International Risk Assurance, Consulting, Cyber Security and Forensics

Göran Laxén (Sweden)
+46 (0)10 2131929
goran.laxen@se.pwc.com

Leda Bargiotti (Belgium)
+32 2 710 4791
leda.bargiotti@be.pwc.com

Tomas Clemente Sanchez (Belgium)
+32 2 7104160
tomas.clemente.sanchez@be.pwc.com

Jay Cline (USA)
+1 (612) 596 6403
Jay.cline@us.pwc.com

Carolyn Holcomb (USA)
+ 1 (678) 419 1000
carolyn.c.holcomb@us.pwc.com

Angela Saverice-Rohan (USA)
+1 (213) 270.8913
angela.m.saverice-rohan@us.pwc.com

Bram Van Tiel (Netherlands)
+31 88 792 5388
bram.van.tiel@nl.pwc.com

Steven Ackx (Belgium)
+ (0) 32 47863 9165
steven.ackx@be.pwc.com

Grace Guinto (Australia)
+61 (3) 8603 1344
grace.guinto@au.pwc.com

Andrew Parker (New Zealand)
+64 (0)4 462 7104
Drew.x.parker@nz.pwc.com

Robyn Campbell (New Zealand)
+64 (0)4 462 7092
robyn.k.campbell@nz.pwc.com

Javier Pérez García (Spain)
+34 682 780 947
Javier.perez.garcia@es.pwc.com

Rajinder Singh (India)
+919873264886
Rajinder.singh@in.pwc.com

www.pwclegal.co.uk