www.pwclegal.co.uk

Privacy and Security Enforcement Tracker 2015

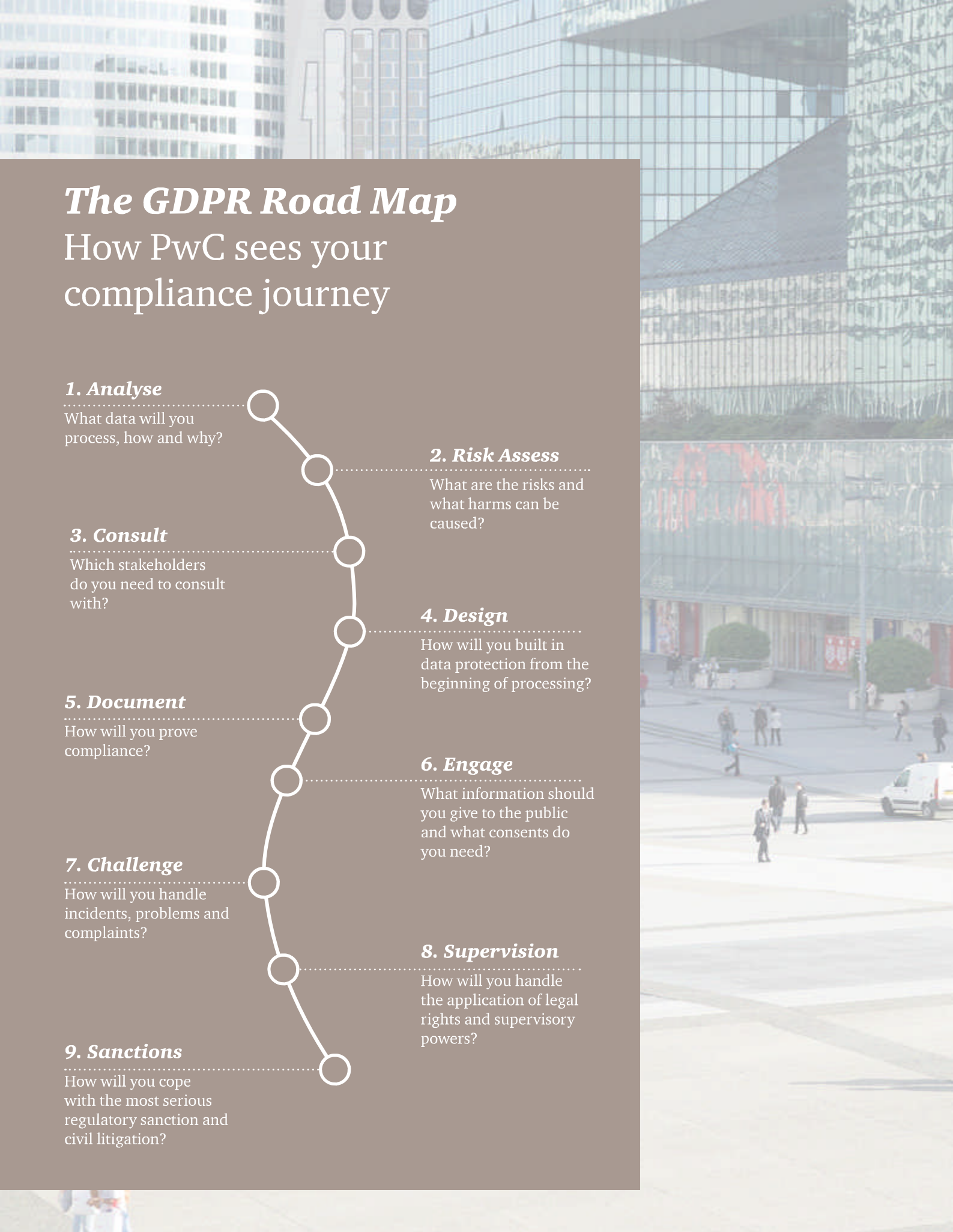
M

pwc

PricewaterhouseCoopers Legal LLP

The GDPR Road Map

How PwC sees your compliance journey



1. Analyse

What data will you process, how and why?

2. Risk Assess

What are the risks and what harms can be caused?

3. Consult

Which stakeholders do you need to consult with?

4. Design

How will you built in data protection from the beginning of processing?

5. Document

How will you prove compliance?

6. Engage

What information should you give to the public and what consents do you need?

7. Challenge

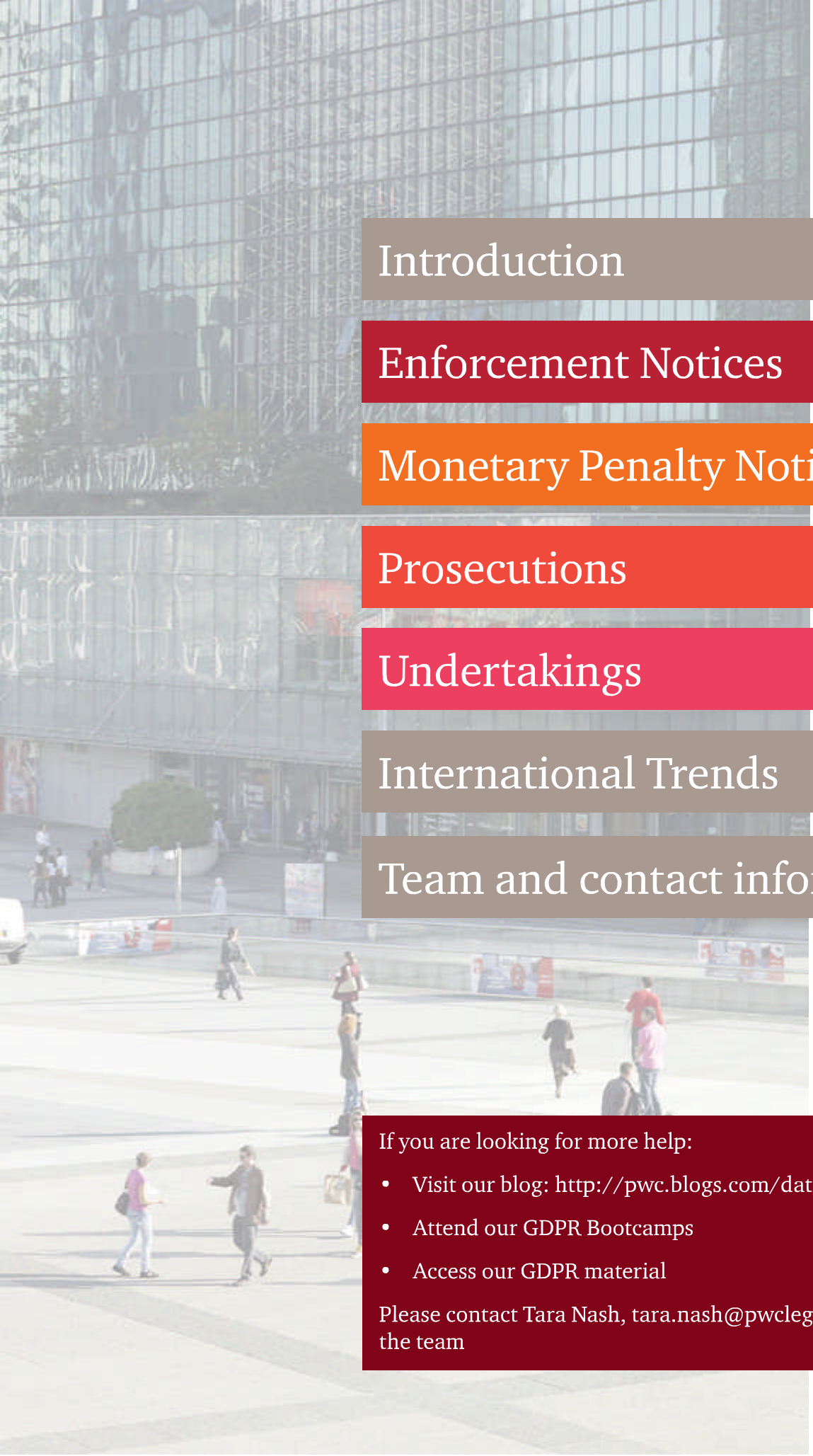
How will you handle incidents, problems and complaints?

8. Supervision

How will you handle the application of legal rights and supervisory powers?

9. Sanctions

How will you cope with the most serious regulatory sanction and civil litigation?



If you are looking for more help:

- Visit our blog: http://pwc.blogs.com/data_protection/
- Attend our GDPR Bootcamps
- Access our GDPR material

Please contact Tara Nash, tara.nash@pwclegal.co.uk or any member of the team

2015, the year when the final alarm was sounded: change, or be changed

Welcome to the second annual PwC Privacy and Security Enforcement Tracker, where we review the previous year's key regulatory enforcement cases in the UK and in twenty other countries.

Twelve months ago we published the 2014 Tracker, calling that year the year of citizen, regulator and judicial activism. Our key message was that privacy and security breaches were being subjected to increasingly adverse, active scrutiny. If 2014 sounded an alarm to encourage the controllers and users of networks, computer and communications systems and personal to review and improve their practices for privacy and security, then 2015 was the year when the final alarm was sounded.

The message of 2015 is clear: entities that fail to take voluntary action to remedy bad practices will be forced to change.

Safe Harbour and the Privacy Shield

Last October the EU Court of Justice delivered its judgment in the Safe Harbour case, bringing to an end a long standing political accord that allowed the transfer of personal data from Europe to the United States. This was an international news story, which put the concepts of privacy and security before a brand new, global audience. The backdrop to the case was Edward Snowden's disclosures in 2013, about how US intelligence agencies were gaining access to European personal information held by US technology companies. The case was brought by a privacy activist, who has taught the world an important lesson: ***one individual is able to rely upon another's whistleblowing, to deliver devastating change to established norms, simply by using privacy laws, litigation tools and the courts.***

The quantifiable change that we already understand includes: change to ***United States*** surveillance practices and US legislation about judicial redress; the creation of a new "Privacy Shield", which replaces the Safe Harbour scheme (with tougher, new regulatory oversight of transfers of personal data to the US); and change to the regulatory mentality in Europe (the European Data Protection Authorities now know that they are legally obliged to properly investigate claims of bad practices in the handling of personal information).

The non-quantifiable change is the effect on the minds of people who are not part of the natural community of privacy activists, security and privacy professionals, regulators, lawyers, judges and politicians whom we can expect to be engaged by privacy and security issues. The Snowden/ Safe Harbour saga has helped to place privacy and security issues into the consciousness of "ordinary" consumers and business people. There are bound to be wider consequences.

Perhaps a good illustration is the case in the US, involving the iPhone. The FBI is seeking access to data on an iPhone owned by a terrorist, but the court order is being resisted. Many representati

the FBI. Arguably, the business mentality has been changed by Snowden/ Safe Harbour.

GDPR and other legislative change

In December 2015 the EU reached a political agreement on the ***General Data Protection Regulation***, after four long years of argument and debate. This followed swiftly on the heels of

the agreement on the ***Cyber Security Directive***. These laws will mandate root and branch change to the way that privacy and security issues are handled, not just in Europe, but also further afield. Entities that refuse to obey will be forced to change by the citizen, regulator and judicial activists, who will all get new powers. Citizens will be empowered with new rights against the controllers and users of personal data, which they will be able to pursue before the regulators and before the courts. If they are distressed by how their personal information are being used, they will be able to sue for compensation. The regulators will be able to order entities to change their practices, which they will be able to back-up with financial penalties on companies of up to 4% of annual worldwide turnover.

Change will be achieved not only through litigation, regulatory action and the imposition of financial pain. The GDPR and the Cyber Security Directive will require entities to disclose security breaches. Bad publicity will damage trust, confidence, brand and reputation. These are powerful drivers.

It is not just Europe that is legislating for privacy and security. As you will see, ***Canada, China, Japan*** and ***Russia*** all introduced new laws to bolster protections in these areas.

Enforcement fines and other sanctions

The trend of regulatory law for privacy and security continues to be in the direction of imposition of financial penalties. The ***UK*** regulator was one of Europe's most prolific finers, which might be a surprise. ***France***, ***Germany*** and ***Italy*** fined too, but on current projections ***Spain*** delivered the most fines in Europe last year. Outside of Europe, Canada imposed some hefty fines and ***Mexico*** and ***New Zealand*** got in on the act too, but the toughest regulatory enforcement regime judged by fines imposed was the ***United States***. In 2015 the US imposed fines totalling $164 million.

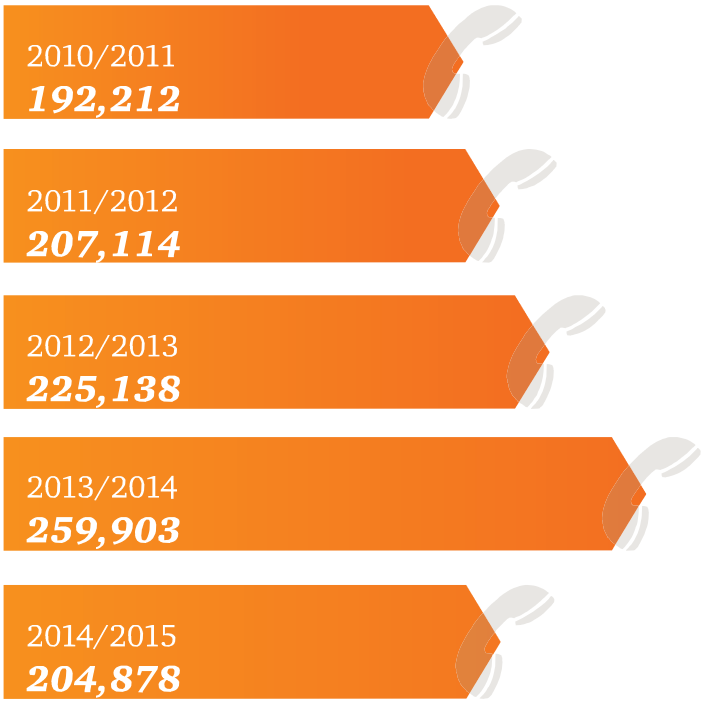
Fines, however, are not the only measure of regulatory "toughness". The volume of cases investigated by the regulators is also an important measure, as is the number of formal enforcement actions. ***Australia's*** regulator dealt with 2000 cases. The number of formal enforcement actions in ***Sweden*** was comparable with the ***UK***. Increases in the frequency of privacy litigation was very noticeable too. There was high profile litigation in ***New Zealand, Austria***, the ***UK*** and ***Belgium***.

Hot topics

The cases and developments in the Tracker identify the hot topics that we all need to be aware of. A short selection will give a flavour of the breadth of regulatory concern: anonymization; security cookies; marketing suppression; web search; dating websites; CCTV surveillance; privacy notices; publishing medical data online; parental consent; subject access requests; accessing social network data; medicine prescriptions data; credit reference data; employee vetting; secure authentication and robocalls. Plainly, we all have a lot to consider.

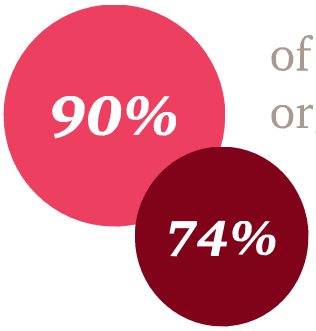
Stewart Room
Partner
Global Head of Cyber Security and Data Protection
PwC Legal
+44 (0) 20 7213 4306
stewart.room@pwclegal.co.uk
@StewartRoom

Helpline calls received by ICO:



(Source: Information Commissioner's Annual Report and Financial Statements 2013/2014, Effective, efficient – and busier than ever, July 2014 and Information Commissioner's Annual Report and Financial Statements 2014/2015)

Levels of security breaches in 2015



of large organisations

of small organisations

had a security breach

▲ Up from 81% a year ago

▲ Up from 60% a year ago

(Source: HM Government and PwC, Information Security Breaches Survey 2015)

Enforcement activities in 2015 by sector

Enforcement in the UK: comparing 2015, 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
2015	18	11	9	25	63

Cost of security breaches in 2015

£1.46m - £3.14m is the average cost to a large organisation

£750k - £311k is the average cost to a small business

of its worst security breach of the year

▲ Up from £600k - £1.15m a year ago

▲ Up from £65k - £115k a year ago

(Source: HM Government and PwC, Information Security Breaches Survey 2015)

Enforcement Notices

Total	***9***
Public Sector	***3***
Private Sector	***6***

North Tees and Hartlepool NHS Foundation Trust

27 February 2015

No Monetary Penalty

DPA – 7th Principle

The Trust was involved in several incidents involving the loss or unauthorised disclosure of personal data; including one where a folder containing sensitive personal data was left at a bus stop and discovered by a member of the public and a number where documents containing personal data had been addressed to the wrong recipient, commonly due to staff overtyping previous patient letters. At least one department within the Trust had been consciously breaching the rules regarding secure transportation of documents contained in the Trust's Data Protection Policy as it felt they were impractical. A previous ICO recommendation letter had highlighted these points but the Trust had failed to effectively implement the recommendations.

Enforced remedial action required within 3 months:

1. Review the Trust's Data Protection Policy, considering the impact on the Trust's departments and how to minimise and secure any personal data stored or transported in or away from the office.
2. Create an action plan to carry out comprehensive quality assurance and spot checks to ensure unilateral compliance with all the Trust's Policies relating to personal data.
3. Implement additional technical or organisational measures to ensure procedures are adhered to by all staff dealing with patient correspondence.
4. Establish a data breach management policy covering the containment and secure retrieval of information.

H

– Regulations 22 & 23

Between 15 December 2013 and 3 April 2014, the Commissioner GSMA's spam text reporting service received 659 complaints from individuals regarding unsolicited marketing text messages. Information as to the identity of the person on whose behalf the communications had been sent was not provided in the message but the Commissioner was satisfied they were sent or instigated by Help Direct.

Enforced remedial action required within 35 days:

1. Unless Help Direct has obtained an individual's contact details in the course of a sale (including negotiation) of a product/ service and the marketing is related to similar products/ services, and there is an option for the individual to refuse direct marketing, Help Direct cannot transmit or instigate unsolicited electronic direct marketing communications unless the recipient has notified Help Direct that they consent.
2. Help Direct cannot transmit or instigate electronic direct marketing communications unless Help Direct is clearly identified as the sender.

5 out of 9 ...

Enforcement Notices issued in 2015 were for unsolicited marketing communications

3

Enforcement Notice and Monetary Penalty Notice combinations (Help Direct, Nuisance Call Blocker, Telecom Protection Service Ltd.)

Sweet Media Limited

23 March 2015

No Monetary Penalty

PECR – Regulations 22 & 23

Between 23 July and 25 May 2014, the Commissioner and GSMA's spam text reporting service received 796 complaints from individuals regarding unsolicited marketing text messages. No sender identification information was included in the messages, but the Commissioner was satisfied the messages were sent or instigated by Sweet Media.

Enforced remedial action required within 35 days:

1. Unless Sweet Media has obtained an individual's contact details in the course of a sale (including negotiation) of a product/ service and the marketing is related to similar products/ services, and there is an option for the individual to refuse direct marketing, Sweet Media cannot transmit or instigate unsolicited electronic direct marketing communications unless the recipient has notified Sweet Media that they consent.
2. Sweet Media cannot transmit or instigate electronic direct marketing communications unless Sweet Media is clearly identified as the sender.

The Department of Finance and Personnel for Northern Ireland (DFPNI)

2 June 2015

No Monetary Penalty

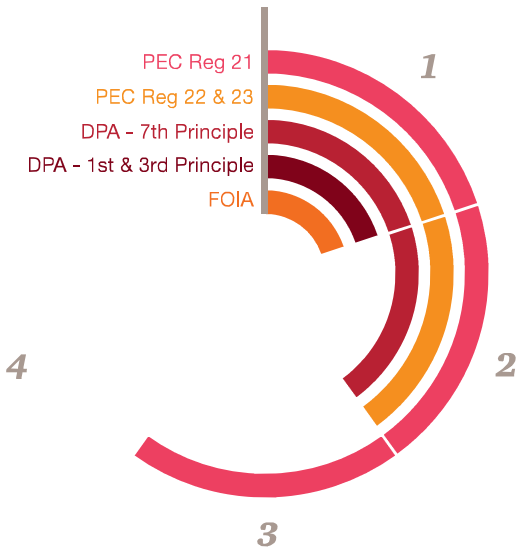
FOIA - Ss. 1 & 10

DFPNI were contacted by the Commissioner on several occasions between May and October 2014 regarding late responses to freedom of information requests. The DFPNI were warned that enforcement action would follow in 6 months' time if improvements had not been made. By March 2015 a number of requests remained outstanding, some by as much as 6 months. As a result of these findings, the DFPNI were formally monitored for 3 months and informed that any outstanding requests over 6 months old should be responded to by 30 April 2015. In May 2015, DFPNI admitted that there were still outstanding requests.

Enforced remedial action required within 30 days:

In respect of each outstanding information request:

1. Inform the individual making the request whether the DFPNI holds the information requested and communicate such information to the individual; or
2. Issue a refusal notice in accordance with s.17 FOIA.



Breach summary - reasons for Enforcement Notices in 2015

1 Enforcemant notice issued in 2015 was related to FOIA

Google Inc.

18 August 2015

No Monetary Penalty

DPA – 1st & 3rd Principles

The Google Spain case (C-131/12) established that internet search engines are data controllers, and that individuals have a right to request them to delist results displayed following a search of their name, where this processing is incompatible with the Directive. A complaint was made to the Commissioner after Google refused to remove links to websites which gave details of a previous de-listing, including the content of the original story relating to a criminal offence, which had been removed by Google following a request from the complainant. Google refused to remove the links on the grounds that they were still relevant and in the public interest. The Commissioner applied the criteria to be used in delisting and decided that Google should remove the links. Google again refused to do so.

The Commissioner held this was a contravention of Google's data protection obligations due to relevant factors such as the individual not being in public life, the personal data was sensitive, the information was not reasonably current as it related to a conviction almost 10 years ago, the processing was having a disproportionately negative impact on the individual's privacy, the public interest could be satisfied without the links, and the criminal offence in question was relatively minor.

Enforced remedial action required by 25 November 2015:

1. Remove links to the websites identified in the Enforcement Notice from the results displayed following a search of the complainant's name, where these results are produced in the context of the activities of Google UK Ltd or any other Google company established in the UK.

Isle of Anglesey County Council

1 October 2015

No Monetary Penalty

DPA – 7th Principle

Following two earlier security incidents, the Commissioner had issued the Council with Undertakings in January 2011 and December 2012. Two audits carried out by the ICO in July 2013 and October 2014 revealed that the Undertakings had not been fully implemented by the Council. On 5 August 2015 the Commissioner issued a Preliminary Enforcement Notice. After considering the Council's representations and in light of their previous record, the ICO only had limited confidence in the Council's commitment to implement the required steps on an ongoing basis.

Enforced ongoing remedial action required within 3 months:

1. Monitor and act on data protection KPI's and measures (including security incidents).
2. Ensure there is a mandatory data protection training programme for all staff (including new starters) and refresher training on an annual basis.
3. Monitor and document completion of such training.
4. Ensure policies (including the Records Management Policy) are being read, understood and complied with by all staff.
5. Back-up information to the external server on a daily basis.
6. Test back-ups periodically to ensure they have not degraded and that information is recoverable.
7. Revoke physical access rights promptly when staff leave and periodically review to ensure appropriate controls are in place.
8. Address the lack of adequate storage solutions for manual records.
9. Undertake consistent and regular monitoring to enforce a clear desk policy.

3

Enforcement notices received a monetary penalty notice

1 enforcement notice was issued to an individual, not a business entity

Nuisance Call Blocker Ltd

19 November 2015

MPN issued on 19 November 2015 of £90,000

PECR – Regulation 21

The Commissioner received a number of complaints via the Telephone Preference Service (TPS), and directly from individuals who were subscribers to specific telephone lines, in relation to unsolicited marketing calls from the company after previously notifying them that such calls should not be made on that line and/or had registered their number with the TPS.

Enforced remedial action required within 35 days:

1. Neither use, nor instigate the use of, a public electronic communications service for the purpose of making unsolicited calls for direct marketing purposes where the line called is that of a subscriber who has:
   i. notified the company that such calls should not be made on that line; and/or
   ii. registered with the TPS at least 28 days prior to such call and has not notified the company that they do not object to such calls.

Telecom Protection Service Ltd (t/a Telecom Preference Service)

19 November

MPN issued on 19 November 2015 of £80,000

PECR – Regulation 21

The Commissioner received a number of complaints via the TPS, and directly from individuals who were subscribers to specific telephone lines, in relation to unsolicited marketing calls from various individuals acting on behalf of Telecom Protection Service (trading as Telecom Preference Service) after previously notifying the company that such calls should not be made on that line and/or had registered their number with the TPS.

Enforced remedial action required within 35 days:

1. Neither use, nor instigate the use of, a public electronic communications service for the purpose of making unsolicited calls for direct marketing purposes where the line called is that of a subscriber who has:
   i. notified the company that such calls should not be made on that line; and/or
   ii. registered with the TPS at least 28 days prior to such call and has not notified the company that they do not object to such calls.

Mr Aurangzeb Iqbal

3 December 2015

No Monetary Penalty

PECR – Regulation 21

The Commissioner received a number of complaints via the TPS, and directly from individuals who were subscribers to specific telephone lines, in relation to unsolicited marketing calls from various individuals acting on behalf of Mr Iqbal after previously notifying Mr Iqbal's representatives that such calls should not be made on that line and/or had registered their number on the TPS.

Enforced remedial action required within 35 days:

1. Neither use, nor instigate the use of, a public electronic communications service for the purpose of making unsolicited calls for direct marketing purposes where the line called is that of a subscriber who has:
   i. notified Mr Iqbal that such calls should not be made on that line; and/or
   ii. registered with the TPS at least 28 days prior to such call and has not notified the company that they do not object to such calls.

3 instances...

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

Monetary Penalty Notices (MPNs)

Total	***18***
Private Sector	***15***
Public Sector	***3***
Total Value	***£2,031,250***

Staysure.co.uk Limited

20 February 2015

£175,000

DPA – 5th and 7th Principle

Staysure, an online travel insurance company, suffered a security breach to their website, which enabled attackers to have access to Staysure's entire customer database. This included names, addresses, card details (including CVV) and medical screening results of its 3 million customers. From this database, 11,096 live card details were targeted by the attackers and around 5,000 of these were subsequently used in fraud. Vulnerabilities in the software used by Staysure had previously been published, but as Staysure had no policy to review and apply software updates they were not guarded against the attack. The company also contravened industry standards by storing CVV numbers.

Aggravating factors:

1. Effect of the contravention: there was evidence that some of the stolen personal data was used for fraudulent transactions.
2. Behavioural issues: Staysure should have been aware of the vulnerability.
3. Impact on the company: Staysure is a limited company with sufficient financial resources to pay a monetary penalty without causing undue financial hardship.

Mitigating factors:

1. Nature of the contravention: Staysure's systems were subject to a criminal attack, the first it had experienced.
2. Behavioural issues: Staysure was in the process of revamping its IT infrastructure and the company voluntarily reported the incident to ICO, taking appropriate remedial action in the first instance while cooperating with ICO.

Remedial Action:

No mention of remedial action.

76% increase in the total value of monetary penalty notices in 2015 when compared to 2014

Serious Fraud Office

26 March 2015

£180,000

DPA – 7th Principle

Following the conclusion of a high-profile investigation into serious fraud, bribery and corruption, the Serious Fraud Office (SFO) began to return the 11,000 bags of evidence to the parties involved. The SFO returned a number of bags to an individual who claimed some of the information in the bags did not belong to him. Following a consideration of the concerns, the SFO were satisfied that no error had been made when returning the bags and continued the process of returning material to the individual, which included confidential personal data relating to around 6,000 data subjects, some of whom were high profile individuals.

Following a briefing requested for a 'Parliamentary Question' the SFO confirmed that some of the further bags had been disseminated incorrectly or could not be located. It was established that a temporary worker was responsible for the errors that resulted in 407 bags belonging to 64 parties (including the suspect of the investigation) being sent to the incorrect party. However, it was found that the worker was inexperienced, had not received sufficient training, was not appropriately supervised, and did not fully understand what was required in such a complex project.

Aggravating factors:

1. Effect of the contravention: some information may have been disclosed to a national newspaper or disseminated overseas.
2. Behavioural issues: the initial concern raised should have made the SFO aware that there was a risk of contravention.
3. Impact on the data controller: this independent government department would bear the liability rather than an individual, and has access to sufficient financial resources.

Mitigating factors:

1. Nature of the contravention: there had been no previous similar breach.
2. Effect of the contravention: almost all the information was recovered by the SFO and the recovered bag seals were intact.
3. Behavioural issues: the SFO voluntarily reported the incident and launched a full and prompt investigation while cooperating with the ICO, making attempts to recover the information from the recipient and taking remedial action.
4. Impact on the data controller: the SFO's reputation would be significantly impacted.

Remedial Action:

1. No mention of remedial action.

Direct Assist Limited

26 March 2015

£80,000

PECR – Regulation 21

Direct Assist Limited, a personal injuries claims company, was the subject of over 800 complaints via the Telephone Preference Service (TPS) hotline and direct complaints to the ICO for making unsolicited calls for direct marketing purposes. All complaints were from data subjects registered with the TPS and who therefore had expressed the preference not to receive direct marketing communications.

Several complaints detailed substantial distress caused to elderly, disabled and otherwise vulnerable data subjects. Other complaints concerned the aggressive and rude manner of calls and inappropriate number of calls, with two households allegedly having been called 470 times.

The ICO and Direct Assist were in dialogue throughout the complaints period from 1 January 2013 to 31 July 2014. However, Direct Assist failed to provide adequate information to the ICO and in some instances the information provided was dishonest. In some instances, Direct Assist claimed they were under the impression that telephone number lists bought from suppliers had been screened. Direct Assist also failed to take appropriate action under the PECR; staff were not trained to ensure compliance and were even instructed to deliberately use telephone numbers from those on the TPS list.

Direct Assist has since gone into liquidation and the ICO is a creditor in the winding-up proceedings.

Aggravating factors:

1. Nature of the contravention:
   i. Complainants received calls after expressing their preference to be removed.
   ii. Any controls Direct Assist claimed were being implemented were since discovered to have been ineffective.
   iii. Direct Assist allegedly withheld their number from some calls in contravention of Regulation 24 of the PECR.
2. Behavioural issues:
   i. Failure to engage with the ICO in a productive dialogue despite having the option extended several times.
   ii. A 'complete disregard' for the law by failing to change business practices and to use the TPS list effectively despite complains made to it by the TPS.
   iii. No reasonable steps taken to ensure staff compliance with PECR, or that bought-in lists were screened properly and instructions were given to staff to disregard the directions of the PECR.
   iv. Rude and aggressive calls were reported.
3. Impact on the company: non-compliance created an unfair advantage for Direct Assist in a competiti

t Direct Assist believed 'bought-in' telephone number lists were properly screened.

2. Impact on the company: significant financial impact and reputational damage.

Remedial Action:

1. No mention of remedial action.

increase in the number of MPNs issued in 2015 when compared to 2014.

Take our GDPR RAT

(Readiness Assessment Tool)

- ***60*** questions
- ***1*** maturity matrix
- ***2*** pillars
- ***1*** hour

Gives you full insight into your GDPR readiness

The Chief Constable of South Wales Police

11 May 2015

£160,000

DPA – 7th Principle

In August 2011, an investigating officer lost three unencrypted DVDs containing a recording of an interview conducted on a victim of sexual abuse as a child. The content was graphic and distressing and the victim was visually identifiable. There was no policy in place for storage of recordings despite there being specific guidance available for Chief Police Commissioners. The DVDs were in fact stored in a shared desk in a keypad-locked area of the police station.

As there was no policy for reporting data breaches, the Chief Constable of South Wales Police was not aware of the breach until August 2013. The trial of the case was at this time ongoing and the loss of evidence had the potential to severely impact the case. The victim was informed of the security breach and made a formal complaint to the Chief Constable of South Wales Police. Both defendants in the trial were eventually found guilty, but the DVDs have not been recovered to date and have the potential to cause a great deal of harm to the victim if further disseminated.

Aggravating factors:

1. Effect of the contravention: the loss of the evidence may have adversely affected the CPS' trial and the DVDs have still not been recovered.
2. Behavioural issues: the data controller was not made aware of the loss for almost two years and there was no force-wide policy for storage and management of such evidence.
3. Impact on the organisation: the data controller is a public authority with sufficient financial resources to pay the penalty.

Mitigating factors:

1. Nature of the contravention: no previous similar security breach has been reported, the DVDs were stored in a physically secure part of the police station, and the data on the DVDs have not been accessed or further disseminated to the Commissioner's knowledge.
2. Behavioural issues: the data controller made extensive searches to relocate the DVDs and voluntarily reported the loss to the ICO, cooperating with the investigation at all times.
3. Impact on the organisation: the data controller's reputation would be significantly affected.

Remedial Action:

1. No mention of remedial action.

I (t/a the Money Shop)

6 August 2015

£180,000

DPA – 5th and 7th Principles

In 2014, the organisation suffered the theft of one server, and the loss of another during transportation between offices by a third party courier. The servers contained the personal information and payment card details of local and national customers, including details of the organisation's employees. The lost server was unencrypted as the encryption process had been initiated but had not completed.

The Commissioner questioned the regular physical movement of servers between the organisation's stores as well as the lack of 'safe haven' rooms in some of these stores. These rooms were allegedly used in all stores according to the organisation. However, it was found that in a number of stores, including that which suffered the theft, the safe haven procedure whereby servers should be locked in a separate room when the shop was closed was not adhered to as the shop was too small.

Aggravating factors:

1. The organisation failed to identify the risk of a lack of wholesale encryption until 2013, and subsequently failed to address this risk.
2. 56 complaints were received about the theft incident.
3. As a limited company, liability does not fall on only one individual.

Mitigating factors:

1. Voluntary reporting to and full cooperation with the Commissioner.
2. Independent consultants were instructed to conduct an internal investigation into the server that was stolen.
3. The data on the lost server was partially encrypted.
4. The organisation contacted customers affected by the losses and offered financial protections to these individuals.
5. No evidence of further third party use of the lost data.
6. The FCA conducted an investigation into the breaches.
7. There have been no other reported incidents.
8. There will be a significant impact on the organisation's reputation as a result of the breach, and the incident was publicised.

Remedial Action:

1. The organisation took substantial remedial action.

Point One Marketing Limited (t/a Stop the Calls)

5 August 2015

£50,000

PECR – Regulation 21

Between February 2014 and March 2015 Stop the Calls (StC) made over 700 unsolicited calls for direct marketing purposes, selling a call blocking service together with an unsubscribe feature to stop unsolicited calls, to recipients who registered with the TPS opt out list, and other related opt out lists. StC consistently appeared on the TPS' 'name-and-shame' top 20 offenders list. StC had also purchased personal data from a third party without undertaking due diligence.

Many of the individuals who reported StC to the Commissioner stated they had felt substantially distressed or harmed by intrusive and aggressive calls, in some instances elderly and vulnerable individuals felt pressured into handing over credit card information. After repeated warnings and a period of monitoring, the Commissioner took enforcement action, finding StC's actions to constitute multiple deliberate breaches of Regulation 21 of the PECR.

Aggravating factors:

1. StC may obtain a commercial advantage by using leads obtained from unlawful marketing practices.

Mitigating factors:

1. StC fully cooperated with the ICO investigation.
2. There will be potential damage to StC's reputation as a result of the incident which may affect future business.

Remedial Action:

1. Some remedial action taken by StC.

Cold Call Eliminations Ltd

14 September 2015

£75,000

PECR – Regulation 21

Between 14 June 2013 and 31 March 2015, Cold Call Eliminations (CCE) made 382 unsolicited calls for direct marketing purposes to recipients registered with the TPS opt out list. CCE called individual subscribers to market a call blocking device and service to stop unsolicited calls. It was found that CCE had purchased data from a third party and did not screen this data against the TPS opt out list. After repeated warnings and two periods of monitoring by the ICO, the drop in the number of complaints to the TPS was small but insignificant. CCE appeared on the TPS' 'name-and-shame' top 20 offenders list on numerous occasions.

The Commissioner found that false and misleading statements were made as to the identity of the business and the nature of the product or service. Many of the calls were made to elderly or vulnerable subscribers and bank details were obtained under duress. Given the number of affected individuals, the Commissioner found it was inherently likely that at least a small proportion would suffer substantial distress on account of their particular circumstances. As the issue of unsolicited calls was widely publicised by the media, CCE should have been aware of their responsibilities.

Aggravating factors:

1. CCE obtained a commercial advantage by using leads obtained from unlawful marketing practices.
2. False and misleading statements were made during calls.
3. Elderly and vulnerable individuals were misled to purchase services from CCE.

Mitigating factors:

1. CCE fully cooperated with the investigation.
2. There will be potential damage to CCE's reputation as a result of the incident which may affect future business.

Remedial Action:

1. No mention of remedial action.

Common aggravating features leading to higher fines:

- Minimal engagement with the ICO
- Significant financial resources
- Obtaining comercial advantage
- Failure to cooperate
- Having received complaints without taking action

Common mitigating features leading to reduced fines:

- Co-operation with the ICO
- Voluntary reporting to the ICO
- Potential damage to reputation

Home Energy & Lifestyle Management Ltd

25 September 2015

£200,000

PECR – Regulation 19

Home Energy & Lifestyle Management Limited (HELM), an official provider of Green Deal (a Government backed energy saving initiative) sent automated marketing calls regarding free solar panels to subscribers of the TPS. Between 2 October and 12 December 2014, the ICO received 242 complaints. The calls did not identify the sender and an option to be connected to a person or to be removed from the contact list was not always effective. The ICO contacted HELM to notify them of their obligations under the PECR and the volume of complaints received. HELM confirmed that they would not be running a similar marketing campaign and that the customer records were purchased from reputable suppliers and screened against the TPS. In a further communication, the ICO asked HELM to provide details of the consents relied upon to make the calls to comply with the PECR. HELM explained that they were not aware that a different PECR regulation applied to automated marketing calls so they adopted the same approach as for live calls. HELM admitted that they sent over 6 million automated calls during the marketing campaign, approximately 59,500 of which were made to TPS subscribers.

Aggravating features:

1. HELM may have obtained a commercial advantage by using leads generated from unlawful marketing practices.

Mitigating features:

1. HELM confirmed that they will not run a similar marketing campaign.
2. HELM fully co-operated with the ICO investigation.
3. Potential damage to HELM's reputation as a result of the incident which may affect future business.

Remedial action:

1. No mention of remedial action.

Hutchison 3G UK Ltd

1 October 2015

Notice of intent - £1,000

PECR – Regulation 5A

Hutchison 3G failed to notify the Commissioner within 24 hours of three personal data breaches that had occurred on 21, 23 and 25 July 2015. This notification is mandatroy under Regulation 5A of PECR. The breaches were instead submitted to the Commissioner on 3 August 2015 in their monthly log to the Commissioner for July 2015. Hutchison 3G cited resource issues and technical difficulties with the ICO's online reporting tool as reasons for the reporting delays. The Commissioner was satisfied that Hutchison had sufficient resources to notify within the required time limit and that there were no technical issues affecting the online reporting tool at the time.

Total value of MPNs:

2015 - £2,031,250

2014 - £1,152, 500

2013 - £1,520,000

2012 - £2,430,000

2011 - £541,000

39%

of MNPs in 2015 were due to unsolicited direct marketing calls

Pharmacy2U Ltd

14 October 2015

£130,000

DPA – 1st Principle

Pharmacy2U, the UK's largest NHS approved online pharmacy providing prescription, doctor and health and beauty services, supplied 21,500 customer names and addresses to marketing companies, based on an age breakdown and a list of likely health conditions. Companies that bought the details included a health supplements company that has been cautioned for misleading advertising and an Australian lottery company subject to an international criminal investigation for fraud and money laundering. The ICO investigation found that the online pharmacy had not informed its customers that it intended to sell their details to third party organisations, in addition to sending out its own marketing material. Customers who wanted to opt out of this type of third party data sharing had to log into their account and change the setting to indicate 'no' for selected company data sharing. As the customers had not provided consent for their personal data to be sold on, Pharmacy2U did not have a lawful basis for processing their data.

Aggravating factors:

1. As a limited company, liability for the MPN does not fall on any one individual.

Mitigating factors:

1. Pharmacy2U fully co-operated with the ICO's investigation.
2. There will be a significant impact on Pharmacy2U's reputation as a result of the incident.
3. The contravention was publicised in the media.

Remediation action:

1. Substantial remedial action was taken.

H

– Regulation 22

Between 15 December 2013 and 3 April 2014, 659 complaints were made to GSMA's unsolicited marketing text message reporting service, or directly to the Commissioner, about messages sent by Help Direct. The messages received included topics such as accident claims, bank refunds and finance applications and the campaign used unregistered SIM cards and dongles which the ICO identified as being a method of evading detection by mobile telephone networks' spam detectors. As a result, the ICO issued an Enforcement Notice on 24 February 2015. However, between 7 and 30 April 2015, a further 6,758 complaints were made.

Aggravating factors:

1. Contraventions took place while the Help Direct was subject to a related Enforcement Notice.
2. Help Direct may have obtained a commercial advantage by using leads generated from unlawful marketing practices.

Mitigating factors:

1. There were no mitigating factors.

Remedial action:

1. No mention of remedial action.

Number of MPNs:

2015 - 18

2014 - 11

2013 - 18

2012 - 25

Crown Prosecution Service

2 November 2015

£200,000

DPA – 7th Principle

The CPS had an informal arrangement with a sole trader to edit videos of police interviews so that they could be used in criminal proceedings. Some of the DVDs were delivered using a national courier firm but in urgent cases the sole proprietor would transport them personally using public transport. The DVDs were unencrypted. For some of the time, the sole proprietor used a residential block as a studio to edit the videos. Two laptops used for editing were left out on a desk and stolen from the studio. The laptops held videos of police interviews with 43 victims and witnesses involved in 31 cases, nearly all of which were ongoing and of a violent or sexual nature and included historic allegations against a high profile individual. The laptops were password protected but not encrypted, were recovered eight days after the burglary and, as far as the ICO were aware, had not been accessed by unauthorised third parties.

The ICO found a contravention based on the transportation method of the DVD's, the lack of awareness of security risks posed by editing the videos at the premises, the lack of security guarantees regarding the storage and destruction of the DVDs, the failure to monitor the security measures taken by the sole proprietor and the lack of a DPA compliant contract with the sole proprietor in relation to the processing.

Aggravating factors:

1. The ICO received three complaints from affected individuals who were notified by the CPS.
2. The CPS has sufficient financial resources to pay the monetary penalty without causing undue financial hardship.

Mitigating factors:

1. The CPS voluntarily reported the incident to the ICO.
2. The laptops were password protected.
3. The laptops were recovered after eight days.
4. As far as the Commissioner was aware, the data had not been accessed by an unauthorised third party.
5. The CPS notified the affected individuals.
6. The CPS fully co-operated with the ICO.
7. As far as the Commissioner is aware, there have been no other security breaches.
8. There will be a significant impact on the CPS's reputation as a result of the security breach.

Remedial action:

1. Substantial remedial action has been taken.

Oxygen Ltd

5 November 2015

£120,000

PECR – Regulation 19 and 24

Oxygen Ltd instigated the sending of over 1 million automated marketing calls relating to debt management to subscribers of the TPS without their prior consent. Between 25 March 2015 and 28 April 2015, the Commissioner received 214 complaints about the receipt of these calls, which did not identify the sender but implied that the calls were made as part of a Government initiative. Oxygen Ltd confirmed that the calls were made on behalf of the company by a third party, but claimed that they were informed the calls would be screened against the TPS list and that the list of numbers it had purchased would be 'opted in'.

Aggravating factors:

1. Oxygen Ltd may have obtained a commercial advantage by generating leads from the unlawful marketing practices.

Mitigating factors:

1. There may be potential damage to Oxygen's reputation which may affect future business.

Remedial Action:

1. No mention of remedial action taken.

Over ***60%*** of MNPs in 2015 were due to a breach of PECR

UKMS Money Solutions Limited

17 November 2015

£80,000

PECR – Regulation 22

Between 6 April 2015 and 10 June 2015, 1,405 complaints were made to the GSMA's unsolicited marketing text message reporting service and 37 directly to the Commissioner regarding messages sent from UKMS, a company that provides services to people seeking to claim compensation for mis-sold Payment Protection Insurance. UKMS confirmed that it had sent 1,320,000 messages in the period. UKMS informed the ICO that the data used to send the messages had been purchased from third party suppliers and stated that messages were only sent to individuals who had opted-in to receive them. The Commissioner explained that it was the responsibility of the sender to ensure compliance and held that the consent wording relied upon was not sufficient to amount to consent under the PECR.

Aggravating factors:

1. UKMS may have obtained a commercial advantage by generating leads from the unlawful marketing practices.

Mitigating factors:

1. UKMS fully co-operated with the ICO's investigation.
2. There may be potential damage to UKMS' reputation which may affect future business.

Remedial action:

1. No mention of remedial action.

Nuisance Call Blocker Limited

19 November 2015

£90,000

PECR – Regulation 21

In February 2015, the Commissioner received a large number of complaints about unsolicited marketing calls from Nuisance Call Blocker Limited (NCBL). Their business involved making calls to individual subscribers to market a call blocking device which purported to stop unsolicited calls. The company failed to reply to several communications from the ICO, which resulted in the ICO issuing an Information Notice on 16 October 2015. NCBL failed to comply with this Information Notice and on 30 September 2015 was found guilty in its absence. The Commissioner found that between 7 April 2015 and 22 July 2015, NCBL made 309 unsolicited direct marketing calls to subscribers, who were falsely given the impression that the calls were part of a government backed initiati

-operate with either the TPS or Commissioner.

Mitigating factors:

1. There were no mitigating factors.

Remedial action:

1. No mention of remedial action.

Nearly 9 out of 10 large organisations surveyed now suffer some form of security breach - suggesting that these incidents are now a near certainty. Businesses should ensure they are managing the risk accordingly.

(Source: HM Government and PwC, Information Security Breaches Survey 2015)

Telecom Protection Service Ltd (t/a Telecom Preference Service)

19 November

£80,000

PECR – Regulation 21

Between 26 September 2013 and 24 July 2015, Telecom Protection Service made 839 unsolicited marketing calls made to subscribers. The calls were made to sell 'cold call prevention' products and/or services. The explanations provided to the TPS for making the calls were either 'old data' or no explanation was given. Telecom Protection Service did not respond to communications from the ICO and failed to comply with an Information Notice. The Commissioner found that repeat calls were made to subscribers who had asked for their number to be suppressed, calls were misleading as they gave the impression they were made for official business, some callers were rude and aggressive and preyed on the elderly and vulnerable and some subscribers were put under pressure to provide their bank details.

Aggravating factors:

1. Telecom Protection Service may have obtained a commercial advantage by generating leads from the unlawful marketing practices.
2. There was a failure to co-operate with the ICO.
3. At the date of this Monetary Penalty Notice, the ICO and TPS were still receiving complaints about Telecom Protection Service.

Mitigating factors:

1. There may be potential damage to Telecom Protection Service's reputation which may affect future business.

Remedial action:

1. No mention of remedial action.

50% of imposed MPNs are higher than £100,000

Bloomsbury Patient Network

11 December 2015

£250

DPA – 7th Principle

Bloomsbury Patient Network (BPN) provides a support network for patients diagnosed as HIV positive and is run by three patient representatives. Around 17 February 2014, one patient representative sent an e-mail to between 60 and 200 users on BPN's distribution list who all had HIV. The email addresses were entered into the "to" field instead of the "bcc" field, meaning that the recipients could see the email addresses of all other recipients and were able to infer their HIV status. The patient representative agreed to be more careful in future, however there was no formal guidance or training reminding the patient representative to double check the email fields. BPN did not replace the e-mail account with one that could send separate emails to each user on the distribution list. On 6 May 2014, the same patient representative sent an email to 200 users on the distribution list, again with the email addresses entered into the "to" field in error.

Aggravating factors:

1. BPN received five complaints from affected individuals.
2. BPN did not ask the unauthorised recipients to delete the emails.

Mitigating factors:

1. BPN fully co-operated with the ICO's investigation.
2. BPN apologised to the affected individuals.
3. There will be a significant impact on BPN's reputation as a result of this incident.

Remedial action:

1. Substantial remedial action has been taken.

Telegraph Media Group Ltd

15 December 2015

£30,000

PECR – Regulation 22

The Telegraph, a multi-media news company, sent a marketing communication for a political campaign, along with their normal editorial bulletin, to subscribers of an "editorial content" mailing list. Recipients on the mailing list had subscribed to the editorial bulletin. Some of the recipients had "opted-out" of receiving marketing communications, and the soft opt-in rule did not apply to those who had not "opted-out" as this was a non-commercial promotion. Recipients on the mailing list had not provided specific consent to receive marketing these communications promoting an election campaign.

Aggravating factors:

1. The Telegraph and the ICO received a total of 17 complaints.

Mitigating factors:

1. The contravention was unprecedented.
2. The contravention was unlikely to cause substantial damage or distress to the recipients.
3. The Telegraph fully co-operated with the ICO's investigation.
4. There is potential for significant damage to the Telegraph's reputation as a result of the contravention, which may affect future business.

Remedial action:

1. Substantial remedial action has been taken.

61%

of CEO's are worried about the effect of ***cyber security threats*** on their organisation's growth prospects

(Source: PwC, 19th Annual Global CEO Survey)

79%

...and for the ***insurance sector*** this figure was 79%

Prosecutions

Total	***11***

T

t Lloyds Banking Group, was prosecuted for unlawfully accessing a former partner's bank account.

Action:

Manzoor was fined £250 and ordered to pay a victim surcharge of £25.

Lismore Recruitment Limited

16 April 2015

Recruitment company Lismore Recruitment was prosecuted for failing to notify the ICO of its data processing activities.

Action:

The company pleaded guilty, was fined £375, ordered to pay a victim surcharge of £38 and ordered to pay costs of £774.20.

Consumer Claims Solutions Limited

4 August 2015

Personal injury claims telemarketing company Consumer Claims Solutions Limited was prosecuted for failing to notify the ICO of its data processing activities.

Action:

The company pleaded guilty, was fined £200, ordered to pay a victim surcharge of £20 and ordered to pay costs of £393.

Nuisance Call Blocker Ltd

8 October 2015

Cold calling prevention team Nuisance Call Blocker Ltd was prosecuted for failing to respond to an information notice.

Action:

The company was fined £2,500, ordered to pay a victim surcharge of £120 and ordered to pay costs of £429.85.

Space Systems Ltd

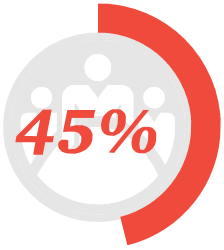
4 November 2015

Storage solutions company Space Systems Ltd was prosecuted for failing to notify the ICO of its data processing activities.

Action:

The company pleaded guilty, was fined £500, ordered to pay a victim surcharge of £50 and ordered to pay costs of £440.

Over **60%** of prosecutions in 2015 were for failing to notify or respond to ICO communications



of boards participate in the overall security strategy

(Source: PwC, The Global State of Information Security® Survey 2016)

Aston James Consulting Ltd (t/a The CV Writers)

13 November 2015

Recruitment company Aston James Consulting Ltd (t/a The CV Writers) was prosecuted for failing to notify the ICO of its data processing activities and for failing to respond to an information notice. Both offences were proved in the company's absence.

Action:

The company was fined £1,250, ordered to pay a victim surcharge of £75 and ordered to pay costs of £619.85.

Direct Security Marketing Ltd and Antonio Pardo

26 November 2015

Lead generation company Direct Security Marketing Ltd was prosecuted for failing to notify the ICO of its data processing activities. The company's sole director, Pardo, was also prosecuted for being negligent in the company committing the offence.

Action:

Both the company and Pardo pleaded guilty. The company was fined £650, ordered to pay a victim surcharge of £65 and ordered to pay costs of £492.78. Pardo was fined £534, ordered to pay a victim surcharge of £53 and ordered to pay costs of £489.08.

Zita Driaunevicius-Cookson

10 December 2015

Driaunevicius-Cookson, a former medical centre practice director, was prosecuted for accessing the medical records of colleagues and their family members without consent.

Action:

Driaunevicius-Cookson was fined £300, ordered to pay a victim surcharge of £20 and ordered to pay costs of £434.73.

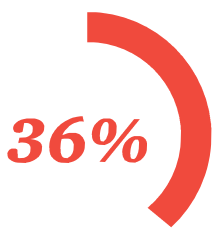
Iheanyi Ihediwa

17 December 2015

Mr Ihediwa pleaded guilty to s55 offences after purchasing nearly 28,000 customer records from Sindy Nagra, an employee of a car rental company. An ICO investigation found that Nagra, who worked from home, had been photographing the records while they were on her computer screen. Nagra was prosecuted separately.

Action:

Ihediwa was fined £1000, ordered to pay prosecution costs of £864.40 and a victim surcharge. The Court also made a destruction order in respect of any data held by Ihediwa.



36%

of prosecutions involved employees' unla l use of personal data at work

Total number of prosecutions:

2015 - 11

2014 - 18

2013 - 7

2012 - 6

Undertakings

Private sector	*7*
Public sector	*16*
Charitable and voluntary	*2*
Total number of Undertakings in 2015	*25*
Follow up reports made in 2015 on Undertakings signed in 2014 and 2015	*17*

Barking, Havering & Redbridge University Hospitals NHS Trust

7 January 2015

DPA – 7th Principle

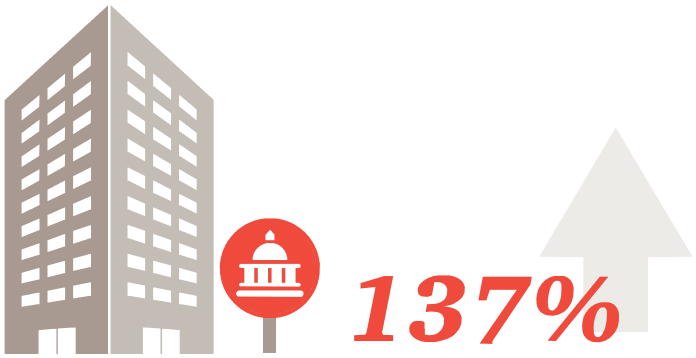
An employee sent faxes containing personal data to an incorrect fax number belonging to a member of the public. Despite the fact that Information Governance (IG) training was mandatory, the employee responsible had not received the training.

Undertakings signed in March 2014:

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

Findings of the ICO on 7 January 2015 in relation to undertakings signed:

1. Annual IG training has been organised and is monitored.
2. Staff must undertake IG training before access to clinical and administration systems is granted.
3. New IG guidance for staff is made available internally.
4. Paper-lite initiative underway.
5. The Trust has taken appropriate steps to address the requirements of the undertaking, but further steps are needed:
   i. Devise a formal framework for the removal of clinical systems access for staff members who have not completed the mandatory training.
   ii. Encourage senior staff to complete training to increase understanding of responsibilities and set an example.
   iii. Ensure contractors complete training.



137%

In 2015, the number of detected security incidents in the public sector increased by 137%

(Source: PwC, The Global State of Information Security® Survey 2016)

Worcestershire Health and Care NHS Trust

13 January 2015

DPA – 3rd and 7th Principles

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

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

Undertakings signed in June 2014:

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

Findings of the ICO on 13 January 2015 in relation to undertakings signed:

1. A procedure for the disposal of confidential information has been implemented and successfully communicated.
2. Information governance and best practice policies have been updated and circulated via appropriate avenues.
3. Training is now mandatory for full time staff, agency staff and support staff.
4. Training includes a short test and staff members receive a booklet.
5. The Trust has taken appropriate steps to and put plans in place to address the undertaking requirements.

Office Holdings Ltd

19 January 2015 & 30 April 2015

DPA – 5th and 7th Principles

A member of the public hacked into an unencrypted database stored on a legacy server. The hacker had access to over a million individual contact details and website passwords belonging to Office customers. Office had several technical measures in place for security but only undertook a single penetration test as the legacy system was to be decommissioned.

Office considered that removal of information before the migration to the new system would be over cautious; an erroneous position in hindsight. In addition, the privacy policy made no reference to retention periods.

Undertakings signed in January 2015:

1. Perform regular penetration testing on all websites and servers.
2. Within three months, implement a new data protection policy to include a retention and disposal policy.
3. Provide formal data protection training and regular refresher courses to all staff.
4. Implement such other security measures as appropriate to ensure personal data is protected.

Findings of the ICO on 30 April 2015 in relation to undertakings signed:

1. A regular penetration testing programme for Office's websites with secondary testing software included has been implemented.
2. Data Protection, Human Resources and Document Retention policies have been introduced and are monitored and reviewed on an ongoing basis.
3. Data protection training including regular refresher training is provided to staff.
4. Security measures have been implemented to ensure data is kept secure and not held longer than necessary.
5. The Company has taken appropriate steps to and put plans in place to address the undertaking requirements, but should ensure the Customer Relationship Marketing database retention period of 5 years/as long as a customer is 'Active' is reviewed.

Google Inc

30 January 2015

DPA – 1st and 2nd Principles

Google proposed a change to its privacy policy in 2012 to streamline around 70 policies into one. This would combine personal data across a variety of services and introduce personal data collection from non-subscribed users of services.

Google entered into dialogue with the Article 29 Working party (WP29) concerning the effect of the new policy. Google subsequently launched the new policy while the WP29 continued its investigation. The ICO raised concerns about the level of information available to subscribers and non-subscribers in relation regarding the ways in which, and purposes for which, service users' personal data is processed.

Suggested changes were not implemented but owing to Google's collaborative and cooperative stance with regulatory bodies the Commissioner decided to require an undertaking in lieu of an enforcement notice.

Undertakings:

1. Compliance with a number of user-focussed clarification and simplification steps.
2. Continued evaluation of the Privacy Policy and associated web content in relation to the reasonable expectations of service users.
3. Continued review of the content of the Privacy Policy and associated web content so users are aware of how their personal data will be processed.
4. Ensure user facing examples are reviewed and relevant.
5. Ensure significant changes to the Privacy Policy are reviewed by user experience specialists.
6. Continue to cooperate with the Commissioner and provide appropriate advance notice of significant changes
7. Report to the commissioner by August 2015 on the steps taken in response to this undertaking.

Findings of the ICO in relation to undertakings signed:

N/A

Approximately ***2/3*** of Undertakings in 2015 were given by public sector organisations

Betsi Cadwaladr University Health Board

11 February 2015

DPA – 7th Principle

Eight letters concerning patients of the Health Board were sent in error to a patient instead of a GP surgery. Six of these letters contained sensitive personal data. The Commissioner found that the employee responsible had not received any formal data protection training.

Undertakings signed in June 2014:

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 2014, all other staff who handle personal data should be trained.
3. Ensure all new staff receive data protection training as part of their induction.
4. Ensure attendance at data protection training sessions is monitored and enforced.
5. Implement such other security measures as appropriate to ensure personal data is protected.

Findings of the ICO on 11 February 2015 in relation to undertakings signed:

1. A training matrix is used to identify staff who handle sensitive information and all on-site identified staff have completed the training.
2. All staff must complete training under the current policy (about a third of all staff have completed an e-learning training module since 2013).
3. The training matrix identifies refresher training delivery.
4. Attendance is monitored during the performance review process and by electronic staff records, with monthly compliance reports sent to a dedicated information governance team.
5. The Board has taken appropriate steps to address the requirements of the undertaking, but further steps are needed:
    i. Ensure remaining staff who handle sensitive information complete the training upon returning to work.
    ii. Ensure a two year refresher program is in place by April 2015.
    iii. Ensure all staff handling sensitive information have completed the training and been enrolled onto the refresher program.

Aberdeenshire Council

23 February 2015

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 signed in June 2014:

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 to be updated at least every three years.
3. Ensure attendance at data protection training sessions is fully monitored.
4. Implement such other security measures as appropriate to ensure personal data is protected.

Findings of the ICO on 23 February 2015 in relation to undertakings signed:

1. Training completion was recorded appropriately and the system regularly identifies staff that have yet to complete the training.
2. By mid-December 2014, 78% of staff undertook the mandatory training; refresher training is available from May 2016.
3. All memory sticks, laptops and smartphones are now encrypted, and security measures to prevent incorrect addressing when communicating data are in place.
4. A process for removing manual records is now in place.
5. The Council has taken appropriate steps to address the requirements of the undertaking, but further steps are needed:
    i. The remainder of staff and any new starters who have not undertaken the mandatory training must do so.
    ii. Staff must complete the refresher training when required and its regularity should be clarified.

92% of Undertakings given in 2015 were related to a breach of the 7th Data Protection Principle (security)

Take our GDPR RAT (Readiness Assessment Tool)

How can we help?

Schedule one hour with one of our privacy experts to undertake our ***GDPR Readiness Assessment*** using our interactive survey.

The survey consists of approximately 60 key questions, with pre-populated answers linked to a Maturity Matrix. Respondents select maturity ratings across a number of dimensions relating to the compliance architecture in place within their organisation, and adherence to the data protection principles contained in the GDPR. The tool produces a report highlighting gaps in your readiness to comply with the GDPR.

The General Data Protection Regulation (GDPR) is a landmark piece of European legislation. It will impact every entity that holds or uses European personal data both inside and outside of Europe.

This GDPR gives rise to increased compliance requirements backed by heavy financial penalties (up to 4% of annual worldwide turnover for groups of companies) and a direct right of action for citizens in European courts. It also contains innovations such as "Privacy by Design", "Accountability" and "Data Portability" and changes the legal parameters of consent. The headline requirements of the GDPR are obvious when you read it, but being able to list them does not necessarily take the organisation forward.

What is more important is an understanding of what the GDPR is really seeking to achieve, what the real risk issues are; how to prioritise compliance activity; and how to build appropriate structures for compliance. The GDPR is seeking to (1) put people back in control of their personal data and (2) improve the protections for personal data at the entity's side. So, at the heart of any compliance programme is a proper understanding of what "good" looks like.

Our GDPR Readiness Assessment Tool has been purpose designed to help our clients to assess where they sit in relation to "good". The findings from the assessment may be used to support the design and build phases of programme development in preparation for complying with the GDPR.

For details of how you can take advantage of this exciting new offering, please contact Emily Thompson or any member of our team.

Emily Thompson
Senior Associate
+44 (0)7802 659 375
emily.thompson@pwclegal.co.uk

South Western Ambulance Service NHS Trust

5 March 2015

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. The Commissioner found there was a lack of data protection training for staff as sending unencrypted discs by recorded delivery posed a security risk.

Undertakings signed in August 2014:

1. Undertake a Privacy Impact Assessment in respect of any data sharing with CCG and other organisations.
2. Ensure appropriate information sharing agreements are in place and maintain a register of agreements.
3. Amend notifications to the ICO to cover the form of processing as well as providing a privacy notice to individuals to reflect this exchange.
4. Ensure all staff undertake data protection training upon starting 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 appropriate to ensure personal data is protected.

Findings of the ICO on 5 March in relation to undertakings signed:

1. PIA's are now completed in any appropriate new circumstance, and new CCG sharing agreements are being developed.
2. All existing information sharing agreements are now listed on the intranet.
3. The new Data Protection Registration identifies that information may be shared with healthcare professionals and leaflets explaining this are provided to patients.
4. Training handbooks are issued to new staff and an online component must be completed within one month.
5. All staff must complete annual training, or specialist training where appropriate.
6. The Trust has taken appropriate steps to address the requirements of the undertaking, but further steps are needed:
    i. The Trust should ensure that the training completion figure reaches at least 95% of all staff.

Approximately ***80%*** of follow up's took place within 6-8 months of the undertaking

Norfolk Community Health & Care NHS Trust

11 March 2015

DPA – 1st, 3rd and 7th Principles

The Trust inadvertently shared data with a referral management centre when files belonging to a third party containing information relating to referrals from health care services for 128,842 data subjects were shared in error.

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

Undertakings signed in September 2014:

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

Findings of the ICO on 11 March in relation to undertakings signed:

1. Increased procedural controls with regard to the transfer of data to third parties have been implemented.
2. Transfers are signed off by the Assistant Director or IM&T and the Trust's Senior Information Risk Owner.
3. Current staff have completed additional training/workshops and training is covered in the information governance induction for new staff.
4. Training is logged appropriately and timely updates are communicated to all staff.
5. The information sharing policy has been updated and a register of information sharing agreements compiled.
6. A review of current contracts was completed to ensure safeguards are in place for the management and protection of data.
7. The Trust has taken appropriate steps to and put plans in place to address the undertaking requirements.

Isle of Scilly Council

13 March 2015

DPA – 7th Principle

In June 2013 an attachment containing unredacted personal data relating to an employee disciplinary hearing was included in error within an email. The recipients were 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. The ICO was also informed of another unauthorised disclosure of sensitive personal data via email occurring in September 2013.

Undertakings signed in September 2014:

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 regularly updated.
3. Communicate guidance 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. Monitor compliance with the Council's data protection and IT security procedures.
6. Implement such other security measures as appropriate to ensure personal data is protected.

Findings of the ICO on 13 March in relation to undertakings signed:

1. A data protection training programme will soon be operational.
2. All staff sharing personal data have access to a new encryption platform.
3. A Redactions Policy and Security Breach Protocol have been drafted.
4. The Data Protection Policy has been reviewed and updated; a new Policy and Scrutiny Officer monitors compliance.
5. The Council has taken appropriate steps to address the requirements of the undertaking, but further steps are needed:
    i. As the training was purchased from another council, this must be adapted to specific needs and policies.
    ii. A monitoring system for training and a schedule for refresher courses should be implemented.
    iii. Guidance on using the encryption system should be provided.
    iv. Appropriate approvals need to be obtained as soon as possible to implement the Redactions Policy and Security Breach Protocol.
    v. The new Information Governance Framework should specify the purpose and role of the Policy and Scrutiny Officer, specifically how the compliance monitoring will be executed.

Gwynedd Council

18 March 2015

DPA – 7th Principle

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

It was subsequently disclosed to the 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 signed in October 2014:

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 provide appropriate training.
3. Implement such other security measures as appropriate to ensure personal data is protected.

Findings of the ICO on 18 March in relation to undertakings signed:

1. Classroom training has continued with refresher courses every three years, and actions taken to provide training to home care staff on induction, first year social workers and students on placements.
2. Policies for the transportation, exchange and use of personal data are covered in classroom-based training, and information management and guidance are communicated in a newsletter and bulletins.
3. Along with the above, briefing notes have been sent to Social Services staff and spot checks of offices are now carried out.
4. A new policy compliance tool will be launched in April 2015 and a Data Protection & Records Management Handbook for social services staff has been drafted.
5. The Council has taken appropriate steps to address the requirements of the undertaking, but further steps are needed:
    i. All staff handling personal data must undertake the mandatory data protection training and monitoring of staff compliance should be implemented.
    ii. Training should be refreshed at least every two years, preferably annually, and the e-learning module should be refreshed annually.
    iii. The Council should determine a set frequency for reminding staff of policies and procedures.
    iv. The Data Protection & Records Management Handbook should be finalised and issued to all staff, and spot checks should be conducted on a regular basis.

Racing Post

16 April 2015

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 the ICO viewed as an unacceptable risk to the security of personal data.

Undertakings signed in August 2014:

By 28 February 2015:

1. Implement appropriate periodic security testing.
2. Implement a secure method of password storage in accordance with industry standards.
3. Define and implement an appropriate software update policy.
4. Regularly monitor compliance with internal data protection and IT security policies.
5. Implement such other security measures as appropriate to ensure personal data is protected.

Findings of the ICO on 16 April in relation to undertakings signed:

1. An Information Security Risk Register has been implemented to identify information security risks in line with ISO27001 controls.
2. A penetration and vulnerability testing policy has been created, with annual systems testing.
3. Adequate proof was provided of technical security for encrypted password storage.
4. A patch management process has been created and updated weekly.
5. New security policies have been implemented which conform to DPA and ISO standards, reviews are regularly undertaken and responsible figures are documented.
6. Training rolled out to senior management.
7. The Racing Post is on track to receive ISO27001 accreditation by early 2016.
8. The Racing Post has taken appropriate steps and put plans in place to address the undertaking requirements and should continue to ensure these are monitored and successfully embedded into their working practices.

Oxford Health NHS Foundation Trust

6 May 2015

DPA – 7th Principle

In May 2013, whilst in the process of creating a new website, a third party contractor unintentionally placed a file containing personal data on the internet relating to approximately 4,200 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 again to blame, 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 signed in September 2014:

1. Put in place adequate data processor contracts (in line with the NHS Information Governance Toolkit) with all third parties processing personal data on the Trust's behalf.
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 Privacy Impact Assessments 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 appropriate to ensure personal data is protected.

Findings of the ICO on 6 May 2015 in relation to undertakings signed:

1. Information governance approval for external supplier contracts involving data processing is now required, with policies and guidance covering this process.
2. New data controller/processor agreements have been implemented.
3. A breach management checklist has been created for incident reporting and senior information governance staff are immediately made aware of incidents.
4. Undelivered mail is now monitored and overseen by the Health Records Department.
5. The Trust has taken appropriate steps to address the requirements of the undertaking, but further steps are needed:
    i. Ensure a revised procurement policy is approved as soon as possible.
    ii. Confirm data processor clauses in contracts are reviewed and established as sufficient.

Pembrokeshire County Council

10 June 2015

DPA – 7th Principle

Following a subject access request, the Commissioner became aware that the Council had incorrectly disclosed a large amount of highly sensitive personal data. Partial redactions had been made but a large amount of information was revealed to the data subject that they were not entitled to receive. The Council had appropriate procedures for a subject access request, but these were not followed due to poor management oversight and a lack of staff training.

Undertakings:

1. Ensure that the relevant procedure is replicated across all areas, implementing suitable changes if appropriate.
2. All staff involved with subject access requests must receive the necessary procedure training to understand the requirements.
3. Ensure proper allocation and oversight of particularly complex requests.
4. Implement such other security measures as appropriate to ensure personal data is protected.

Findings of the ICO in relation to the undertakings signed:

N/A

The number of security breaches has increased, the scale and cost has nearly doubled. 11% of respondents changed the nature of their business as a result of their worst breach.

(Source: HM Government and PwC, Information Security Breaches Survey 2015)

Thamesview Estate Agents Ltd

10 June 2015

DPA – 7th Principle

The estate agent insecurely disposed of personal data by leaving it in the street in transparent refuse sacks whilst waiting for collection by a disposal company. In spite of a warning from the 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.

The Commissioner established that employees were unaware of policies around the disposal of confidential waste. In addition, the estate agent did not have a contract in place with the data processors they used to securely dispose of data.

Undertakings signed in July 2014:

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 appropriate to ensure personal data is protected.

Findings of the ICO on 9 June 2015 in relation to undertakings signed:

1. All staff and applicants are provided with the company handbook, covering data protection, and are required to sign that they have read and understood the requirements.
2. Staff are required to complete best practice sessions after nine months of employment.
3. Offices have been provided with cross shredders to handle daily confidential waste disposal.
4. A Data Handling Policy has been implemented which is reviewed regularly by the coaching and development team, and annually by the data protection officer.
5. Electronic storage by scanning has been introduced to reduce the volume of paper files and to mitigate the associated risk.
6. Thamesview has taken appropriate steps to address the requirements of the undertaking, but further steps are needed:
   i. Staff must complete a data protection course and test annually.
   ii. Contracts with confidential waste disposal companies, and third party software suppliers must contain data protection clauses.

London Borough of Hammersmith and Fulham

11 June 2015

DPA – 7th Principle

A data breach occurred after an incorrectly addressed letter was received by a neighbour of the intended recipient. The letter contained confidential details of the data subject's complaint to a data controller. A further breach was also discovered during the investigation. The Council was found to have acted slowly in recognising the breaches. In addition, the staff responsible for the errors in addressing the letters had not undertaken training within the last few years. Whilst policies were in place, training was left uncompleted by many of the staff.

Undertakings signed on 11 June 2015:

1. By 1 December, ensure that training is completed by all permanent and temporary staff in line with the Council's Data Protection Policy and the requirements of the DPA.
2. By 1 December, implement department-specific refresher programmes to ensure staff are aware of their relevant duties at least every two years.
3. Ensure attendance for training sessions is monitored and procedures are in place to ensure compliance.
4. Implement such other security measures as appropriate to ensure personal data is protected.

Findings of the ICO on 2 December 2015 in relation to the undertakings signed:

1. There is a 91 % completion rate for induction training on data protection.
2. Attendance is monitored for online and face to face training.
3. There is a new information security policy as part of a new information security framework.
4. The development of a course of refresher training has been accepted.
5. The Council has taken appropriate steps to address the requirements of the undertaking, but further steps are needed:
   i. Ensure that that the proposed refresher training is agreed, formalised and implemented across the Council.
   ii. Embed the information security policy across the council through an awareness campaign and staff training.
   iii. Ensure all staff complete the required data protection training.

The Chief Constable of South Wales Police

30 June 2015

DPA – 7th Principle

In August 2011, an investigating officer lost three unencrypted DVDs containing the recording of an interview with a victim of sexual abuse as a child. The content was graphic and distressing and the victim was visually identifiable. There was no policy in place for storage of recordings despite there being specific guidance available for Chief Police Commissioners. The DVDs were in fact stored in a shared desk in a keypad-locked area of the police station. The ICO issued a monetary penalty notice in May 2015 and during oral representations it emerged that action to address the breach remained outstanding. Therefore the ICO determined that an undertaking was necessary.

Undertakings:

1. Ensure that a 'Storage, Custody and Destruction of Visual Recordings' policy is implemented and disseminated to all staff by 30 June 2015.
2. Implement such other security measures as appropriate to ensure personal data is protected.

Findings of the ICO in relation to the undertakings signed:

N/A

(Source: HM Government and PwC, Information Security Breaches Survey 2015)

The Universities and Colleges Admissions Service (UCAS)

14 July & 30 November 2015

DPA – 1st Principle, PECR Regulation 22

An article published by the Guardian newspaper in March 2014 found UCAS to have been providing individuals as young as 13 with an 'opt out' consent to commercial offers by means of direct marketing. These offers were provided alongside educational and health offers and formed part of the same consent. The wording of this consent also implied that data subjects who did not elect to receive the direct marketing communications may miss out on the important health and education news. The relative age and inexperience of the data subjects prompted the ICO to take further action by way of undertakings.

Undertakings signed on 2 April 2015:

1. By the 2016 'entry cycle' application commencement, the online application process should be amended to provide more "granular" information with separate consents for mailings relating to study and career opportunities and health information to direct marketing of commercial offers.
2. By 30 June 2015, the privacy policy and privacy information available to applicants should be amended to provide clear, intelligible and accessible information to users about how their data is processed and who their data is shared with.
3. By 30 June 2015, commit to user testing of privacy policies and privacy information used in the application process.

Findings of the ICO on 14 July and 30 November 2015 in relation to undertakings signed:

1. New commercial mailing "opt-ins" have been launched in all application schemes.
2. Four new "Applicant Declarations" have been produced and approved for admission schemes providing clearer and more in-depth information about the uses of personal data (including sharing).
3. A new privacy policy has been developed and launched on UCAS' website.
4. User testing was conducted and feedback was acted on.
5. UCAS has completed a complete cookie audit and updated their cookies policy.
6. UCAS has reviewed their approach to sharing personal data with third parties and will only provide personal data to bodies with a necessary operational role in the admissions process, unless they have the active and informed consent of applicants.

Western Health & Social Care Trust

15 July 2015

DPA – 7th Principle

In October 2013, two computers were stolen from the premises of the Trust. One computer contained sensitive information relating to mental health services. This information had been deleted but was potentially still recoverable. The ICO determined that additional technical security measures could have been implemented to protect against the theft. Policies were in place to safeguard personal data but these were found to be insufficient.

Separately, a subject access request revealed sensitive data about two individuals not concerned with the request. Their records had been misplaced in the original requested file. Information governance policies and procedures were in place but there was evidence that not all staff were aware of these.

Undertakings:

1. Maintain and assess systems for folder redirections to ensure personal data is securely retained.
2. Review asset control processes to ensure equipment is clear of personal data before redistribution.
3. Ensure that physical security measures are adequate to prevent unauthorised access to personal data.
4. Review guidance, training procedures and policies around subject access requests, specifically where redaction is necessary.
5. Implement mandatory refresher training for all requirements of the DPA and internal policies to staff routinely processing personal data.
6. Implement such other security measures as appropriate to ensure personal data is protected.

Findings of the ICO in relation to the undertakings signed:

N/A

Common themes in Undertakings:

- Requirements for mandatory staff training and refresher courses, including for temporary staff
- Clear policies and guidelines communicated to staff
- Implementing/reviewing policies on subject access requests, data storage, retention and disposal, and checking correspondence
- Security procedures and controls

Rochdale Borough Council

15 July 2015

DPA – 7th Principle

In January 2014 social care files were stolen from the boot of a Council employee's car that was parked in a public place. The files were reported found but contained sensitive data, including criminal sexual offences, of 29 individuals and personal data from many more. The employee was found to have breached the Council's internal policy by removing excessive information from the office.

The Council was found to have insufficient policies in place to train temporary and long term temporary employees, although procedures were given to staff on induction.

Undertakings:

1. Any staff handling personal data must receive data protection training, which must be monitored by the Council.
2. Refresher training in accordance with the Council's policy should be completed by staff and monitored.
3. All agency, temporary and non-permanent staff should receive training in line with the above on an ongoing basis, which should be monitored by the Council.
4. Implement such other security measures as appropriate to ensure personal data is protected.

Findings of the ICO in relation to the undertakings signed:

N/A

King's College London

21 July 2015

DPA – 7th Principle

A spreadsheet of personal data, including exam results, of over 1.800 students was incorrectly sent to a group of students. The document was not checked before it was sent for personal data. It was found that there was an absence of written procedures available to staff to follow and insufficient mandatory data protection training available. A voluntary training scheme had been completed by less than 10% of all staff.

Undertakings:

1. By 31 October 2015, the College must introduce mandatory data protection training for all staff handling personal data, to be refreshed every two years.
2. All staff should complete the training implemented above by 31 December 2015.
3. The College should monitor completion of training with statistics compiled and reported to senior management/ working groups with appropriate follow up for staff who did not complete the training.
4. By 30 September, policies for checking documents for personal data when communicating information to students should be reviewed.
5. Implement such other security measures as appropriate to ensure personal data is protected.

Findings of the ICO in relation to the undertakings signed:

N/A

Total number of Undertakings

2015	2014	2013	2012
25	29	22	31

Parole Board for England & Wales

24 July 2015

DPA – 7th Principle

In September 2013 a dossier of parole evidence carried by a Parole Member was potentially left on a train. The individual was unsure of its status, it may have been shredded, and there was no further confirmation of its whereabouts. The dossier contained sensitive personal information about a prisoner.

The Board has since implemented changes to their guidance on the transportation and destruction of such dossiers but the lack of training offered to Parole Members, as well as the absence of a homeworking policy, encouraged the ICO to require an undertaking to be signed.

Undertakings signed in March 2015:

1. Implement a remote working policy which assesses and records the suitability of sending dossiers to a home environment including the safe storage and handling of documents.
2. Require Parole Members to confirm secure destruction of dossiers through shredding, or provide guidance for additional procedures and checks to be undertaken to confirm destruction where this is not possible.
3. Provide and monitor data protection training for Parole Members, including refresher courses.
4. Implement such other measures as appropriate to ensure personal data is protected.

Findings of the ICO on 24 July 2015 in relation to undertakings signed:

1. Remote working guidance for information assurance has been revised and updated, with tracking built in to determine which dossiers are in Parole Members' possession.
2. Dossier destruction advice forms part of the guidance with an approved courier for collection, or secure destruction on site.
3. Parole Members are required to sign an Information Assurance Declaration annually confirming awareness of Information Assurance, Data Protection and Information Security policies, and the process is monitored by the Board.
4. The Board has increased staff awareness of policies by exhibiting at internal events.
5. A recruitment presentation has been prepared for new members joining the Board.
6. A web access module for remote dossier access is in development, removing the need to carry hard copies and so reducing the risk of loss in transit.
7. The Board has taken appropriate steps to address the requirements of the undertaking, but further steps are needed:
8. The Board should ensure that outstanding declarations from July follow ups are shortly received, emphasising the importance of returning these in a timely manner to Parole Members.
9. The Board should find a technical solution to enable access to the information assurance modules available to Civil Service staff on the Civil Service Learning website.

Community Transport (Brighton, Hove & Area) Limited

27 July 2015

DPA – 5th and 7th Principles

In February 2015 the Community Transport Limited reported the loss of a removable back-up hard drive containing a customer database with over 4,000 records, including sensitive personal data. The member of staff who had taken the drive home subsequently failed to return to work. The Commissioner determined that Community Transport Limited could have taken steps to reduce the possibility of this incident occurring by providing guidance to staff on data protection requirements, implementing an off-site data removal policy and a policy to govern access and storage of personal data. In addition, the Commissioner discovered that Community Transport Limited was retaining data for longer than was necessary and the data stored on removable devices was not routinely encrypted.

Undertakings:

1. Ensure removable and mobile media meet current encryption standards if the data stored is likely to cause damage or distress to individuals.
2. Improve policies relating to the storage and use of personal data.
3. Implement DPA compliant policies to address the retention of personal data.
4. Ensure staff are fully aware of and trained on these policies.
5. Ensure staff handling personal data are given appropriate, specific training when joining Community Transport Limited, to be refreshed regularly.
6. Implement such other security measures as appropriate to ensure personal data is protected.

Findings of the ICO in relation to the undertakings signed:

N/A

While employees still constitue the biggest source of security incidents, incidents attributed to business partners climbed **22%**

(Source: *Key findings from the Global State of Information Security® Survey 2016*)

Cambridgeshire Community Services NHS Trust

29 July 2015

DPA – 7th Principle

After receiving reports of several incidents of losses and theft of personal data, including sensitive data, the Commissioner discovered that the Trust's information governance (IG) training was only required to be taken by staff every two years. The Commissioner's 'IG Toolkit' for citizen care organisations mandated annual training from November 2013. The Trust took steps to introduce annual training, as required, but the uptake was poor with under half of the staff complying with the requirement.

Undertakings:

1. By 31 August 2015, ensure a 95% compliance rate for staff completing IG training.
2. By 30 September 2015, review training provisions to ensure compliance with the Commissioner's 'IG Toolkit'.
3. By 30 September 2015, review the enforcement of completion of staff refresher training, ensuring effective action is taken against offenders.
4. Implement such other security measures as appropriate to ensure personal data is protected.

Findings of the ICO in relation to the undertakings signed:

N/A

Doncaster Metropolitan Borough Council

4 August 2015

DPA – 7th Principle

After the loss of a file containing 66 records following an office move, the Commissioner discovered that staff completion of mandatory data protection was poor. Staff who did complete the training did so only every three years. The official guidance given by the Commissioner recommends that training is completed annually and by all staff in charge of personal data.

Undertakings:

1. Conduct a training needs analysis to determine which positions require more frequent data protection training and refresher training, considering how this can be tailored to suit specific roles.
2. Deliver mandatory data protection training in line with the above analysis.
3. Ensure that staff complete the training within the identified timescales.

Findings of the ICO in relation to the undertakings signed:

N/A

In 2015, ***38%*** more security incidents were detected than in 2014

(Source: Key findings from the Global State of Information Security® Survey 2016)

Key topics from the ***GDPR*** seen in ICO enforcement actions:

1. **Privacy Impact Assessments**
2. **Data sharing**
   - Agreement
   - Register
3. **Accountability**
   - Data Sharing register
   - Demonstrating compliance
   - Accountable officer
   - Importance of training and awareness

Brunel University London

6 August 2015

DPA – 7th Principle

During a repair project the University lost ten boxes containing personnel files, amongst other personal information. The boxes were due to be moved to the Archive and Records Centre and were locked in a room before they went missing. The University had a procedure for staff to follow when transferring files between departments, as well as a retention schedule, but a poor completion rate of internal training led to the Commissioner requesting assurances in this area.

Undertakings:

1. Ensure staff members charged with handling personal information receive data protection training.
2. Implement regular refresher training to staff which is monitored and completed annually.
3. Implement such other measures as appropriate to ensure personal data is protected.

Findings of the ICO in relation to the undertakings signed:

N/A

Anxiety UK

6 August 2015

DPA – 5th & 7th Principles

Personal data, some of which related to anxiety conditions of individuals, held within a password protected area of Anxiety UK's website was publically available for 12 months due to a coding error by a third party website designer. The Commissioner determined that Anxiety UK had failed to ensure the website designer had sufficient technical measures, such as penetration testing, in place to ensure a secure system. In addition, out-of-date membership details were available owing to inadequate quality assurance controls.

Undertakings:

1. Implement appropriate periodic security testing of the website.
2. Implement adequate contractual controls and supporting review mechanisms to ensure compliance of its data processors.
3. Implement appropriate retention, review and disposal controls to ensure that personal data is not held for longer than is necessary.
4. Implement such other measures as appropriate to ensure personal data is protected.

Findings of the ICO in relation to the undertakings signed:

N/A

Over ***half*** of 2015 Undertakings relate to health and local government sectors

British Show Jumping Association

18 August 2015

DPA – 7th Principle

A file containing a large section of the Association's membership database was emailed to a distribution group in error. The file contained the names, dates of birth, contact details and membership details of 14,152 members. The file had been held for longer than necessary and had been given the same name as a file usually sent to the distribution group. The Commissioner found there were no policies and procedures giving appropriate advice to staff on emailing personal data, retention or naming of documents on shared drives. There was also no data protection training given to staff.

Undertakings:

1. Ensure guidance is provided to staff on checking emails containing personal data before they are sent and formalise this guidance in an appropriate policy or procedure.
2. Introduce an appropriate policy or procedure for the use of shared network drives which includes advice on retention and file naming.
3. Implement such other measures as are deemed appropriate to ensure personal data is protected.

Findings of the ICO in relation to the undertakings signed:

N/A

General Dental Council

16 September 2015

DPA – 7th Principle

Fitness to practice allegations, including a CD with background information, were sent in error to a recipient with a similar name to the registrant subject to the allegations. The General Dental Council's (GDC) guidance and checking process was not followed and contrary to the GDC guidance, the CD was not encrypted. The GDC had sufficient written policies in place but there was an absence of refresher training and induction training was not rolled out to existing staff when it was introduced. Masterclasses delivered to individual teams occurred on an ad hoc basis and at least one of the individuals involved in the breach had attended.

A second complaint to the Commissioner, regarding the loss of a set of a patient's dental records, raised similar training concerns.

Undertakings:

1. By 30 September 2015, ensure all current employees who process personal data have received data protection training.
2. By 30 November 2015, set up mandatory refresher training to be updated at least every two years.
3. Ensure the completion of data protection training sessions is monitored and reported to management.
4. Implement such other measures as are deemed appropriate to ensure personal data is protected.
5. The GDC will proactively take the following additional steps:
6. Extend the training programme to include Fitness to Practice panellists and Investigating Committee members, as well as employees.
7. Develop a programme for more targeted training of key groups.

Findings of the ICO in relation to the undertakings signed:

N/A

"***36%*** of businesses now have security strategy for Internet of Things".

(Source: *PwC, Key findings from the Global State of Information Security® Survey 2016*)

Flybe Limited

24 September 2015

DPA – 7th Principle

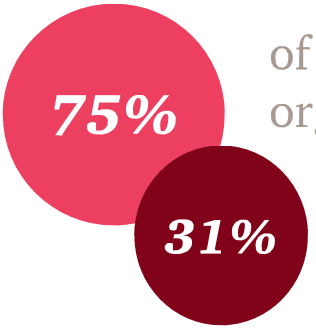
A temporary employee of Flybe emailed a scanned picture of an individual's passport to his personal email account. The Commissioner found that access to various forms of personal data was granted to temporary employees without due consideration to carrying out similar background checks to those used for permanent employees. The Commissioner's investigation found that Flybe did not provide data protection training to all staff members who process personal data and that their Data Protection Policy was inadequate.

Undertakings:

1. Revise the policy covering the storage and use of personal data to outline the different categories of information processed and details on how such data will be protected.
2. Ensure staff are aware of the policy for storage and use of personal data and are appropriately trained.
3. Ensure all staff members handling personal data receive data protection training on induction, to be refreshed annually.
4. Ensure the reliability of temporary employees and where appropriate, bring their checks in line with those for permanent staff.
5. Implement such other measures as appropriate to ensure personal data is protected.

Findings of the ICO in relation to the undertakings signed:

N/A



of large organisations

of small organisations

suffered staff related security breaches in the last year

▲ Up from 58% a year ago

▲ Up from 22% a year ago

(Source: HM Government and PwC, Information Security Breaches Survey 2015)

Martin & Company

24 September 2015

DPA – 7th Principle

Martin & Company, a firm of solicitors, asked a third party to collect a DVD of evidence to be used in a criminal trial from the Crown Office & Procurator Fiscal Service's office. The DVD was mislaid by the third party before being handed to Martin & Company. The DVD's contents were not encrypted. The Commissioner found that although the DVD was not in the possession of Martin & Company, there were a number of shortcomings in the organisation's procedures, such as a lack of guidance to staff regarding data protection training and compliance and a lack of a formal procedure for collecting personal data outside of the office.

Undertakings:

1. Within three months, implement procedures for the collection of items containing personal and sensitive personal data from third parties.
2. Within three months, put in place safeguards to ensure that where appropriate, portable media is encrypted.
3. Within three months, implement a Data Protection Policy setting out how Martin & Company will comply with the DPA.
4. Ensure staff are aware of the policy for storage and use of personal data and are appropriately trained.
5. Ensure staff responsible for handling personal data are given specific training on induction, to be refreshed annually.
6. Implement such other measures as appropriate to ensure personal data is protected.

Findings of the ICO in relation to the undertakings signed:

N/A

Staff training was a key feature in ***80%*** of 2015 Undertakings

Sirona Care & Health

13 November 2015

DPA – 7th Principle

In March 2015, an email containing sensitive personal data about three service users was sent in error by an employee to a previous service user. Sirona became aware of the incident when it was contacted by the unintended recipient, who then deleted the email. Although Sirona did have some data protection policies and procedures in place, these were not fully effective as they did not provide detailed guidance on checking email addresses or deleting those no longer in use. The Commissioner found that the employee had not received governance training for over two years and only 66% of Sirona's staff were up to date with this training. Additionally, the Commissioner held that Sirona may not have taken sufficient steps to act on his previous advice in response to a previous incident.

Undertakings:

1. Ensure mandatory annual data protection refresher training is in place for all staff who routinely process personal data.
2. Ensure the completion rate of data protection training is monitored and implement follow up procedures for staff non-compliance.
3. Review policies to ensure appropriate advice on email checking procedures is provided and readily accessible to staff.
4. Implement such other measures as appropriate to ensure personal data is protected.

Findings of the ICO in relation to the undertakings signed:

N/A

Falkirk Council

23 November 2015

DPA – 7th Principle

On 12 March 2015, Falkirk Council informed the Commissioner of a security breach whereby the Council provided an individual with documents relating to an unconnected third party, which included sensitive personal data, in its response to a subject access request made by the individual. The error was due to the incorrect filing of the third party's documents and a lack of checks on the documents sent to the individual. The Commissioner's investigation found that only 11.4% of Council employees had completed one or more sections of the authority's data protection training modules.

Undertakings:

1. Within nine months, provide mandatory training to all staff members who handle personal data, which will be refreshed annually.
2. Within six months, implement a process for monitoring attendance and completion of data protection training, including steps to be taken for non-attendance. Corporate training KPIs must be reported to and overseen by senior management.
3. Within six months, issue improved guidance to staff members who routinely handle subject access requests, including DPA requirements and how to deal with third party data.
4. Within 6 months, produce a high level Data Protection Policy and communicate this to all relevant staff members within one month of completion.

Findings of the ICO in relation to the undertakings signed:

N/A

The most common ***policies to review*** in Undertakings were:

- Data retention, storage and disposal
- Subject access request procedure
- Correspondence checking
- Privacy Policy

69%

Use cloud-based cybersecurity services

(Source: *PwC, Key findings from the Global State of Information Security*)

Leeds Community Healthcare NHS Trust

25 November 2015

DPA – 7th Principle

The Trust provided the Commissioner with a report that two letters containing sensitive personal data relating to one patient had been included in the response to another person's subject access request. The error occurred as the letters were filed incorrectly and opportunities to identify the wrongly filed letters were missed. The Commissioner's investigation found that temporary staff employed for less than three months may not receive any data protection training, and Information Governance training, which includes data protection, is only refreshed every three years.

Undertakings:

1. Ensure that all staff processing personal data are provided with data protection training before they carry out relevant work.
2. Ensure that data protection training is checked and recorded as part of the induction for new staff members.
3. Ensure that data protection training is refreshed annually where necessary.
4. Ensure that data protection training is fully monitored and attendance enforced where necessary.
5. Ensure that dedicated training is provided to staff handling subject access requests and refreshed annually.
6. Implement such other measures as appropriate to ensure personal data is protected.

Findings of the ICO in relation to the undertakings signed:

N/A

Leverage Big Data analytics for security

(Source: *PwC, Key findings from the Global State of Information Security*)

Northumbria Healthcare NHS Trust

30 November 2015

DPA – 7th Principle

In March 2014 the Trust incorrectly sent a fax to a member of the public which contained the sensitive health data of patients. The Trust was aware of this error, but did not take sufficient steps to prevent a further four faxes being wrongfully sent in May 2014. No attempts were made to check compliance in all wards, and the controls introduced were found to be insufficient on a wider organisational scale.

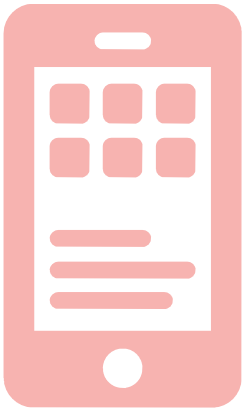
Undertakings signed in May 2015:

1. By 30 October 2015, deliver training and implement procedures to ensure reported security breaches are promptly acted upon and remedial measures are swiftly enforced.
2. By 30 October 2015, implement and regularly monitor a fax policy across all wards which includes proper guidance on the use of safe haven fax machines, to be distributed to staff and regularly monitored.
3. Implement such other security measures as appropriate to ensure personal data is protected.

Findings of the ICO on 30 November 2015 in relation to undertakings signed:

1. Procedures are in place to ensure that reported breaches are promptly acted upon and remedial measures are swiftly enforced, however there is no evidence of staff training.
2. Fax procedures were implemented, however there was no evidence of compliance monitoring.
3. Revised policies and procedures on safe haven fax machines have been circulated to management and will be cascaded to their teams. Warning signs have been put next to all fax machines.
4. The Trust has created solutions to deal with the security problems associated with using faxes.

91%



Use advanced authentication

(Source: *PwC, Key findings from the Global State of Information Security*

South West Yorkshire Partnership NHS Foundation Trust

21 December 2015

DPA – 7th Principle

In July 2013 the Trust disclosed a letter of discharge to an unrelated third party. The 'Safe Haven' policy the Trust had in place did not ensure personal data was checked prior to documentation being sent out. On investigation, the Commissioner discovered four similar incidents had occurred. The Trust had not produced a formal data breach handling policy, instead choosing to inform staff by email, and reminding them of the need to check addresses before sending, and no action was taken against the responsible members of staff.

Undertakings signed in May 2015:

1. Update the 'Safe Haven' policy to cover the checking of contents of correspondence by any medium before sending.
2. Provide a formalised policy containing guidance to staff on checking contact details.
3. Establish a data breach handling investigation and remediation protocol with a clear overview of the steps to take and the timeframe for completion.
4. Implement such other security measures as appropriate to ensure personal data is protected.

Findings of the ICO on 21 December 2015 in relation to undertakings signed:

1. The Safe Haven policy has been updated for validation checks as required and was expected to be ratified in October 2015.
2. Work has begun on developing local processes aligned to the updated validation check procedure guidance.
3. The Trust has reviewed its processes for managing information governance incidents and has amended its incident reporting form.
4. Reported information governance incidents not already graded as amber have been regraded to this mandatory level to ensure they are appropriately investigated.
5. The Trust recently ran a 'Think Information Governance' campaign to raise staff awareness.
6. The Trust has developed new classroom-based information governance training.
7. The Trust has taken appropriate steps to address the requirements of the undertaking, but further steps are needed:
    i. Ensure the updated Safe Haven policy is ratified, made available to staff and awareness of key amendments is raised.
    ii. Ensure local processes for checking the content and contact details of all outgoing correspondence are developed in all areas and included in role-specific training.
    iii. By April 2016, review the Investigating and Analysing Incidents, Feedback and Claims to Learn from Experience Policy.
    iv. Communicate changes to all staff as soon as practicable.

Croydon Health Services NHS Trust

23 December 2015

DPA – 7th Principle

The Trust informed the Commissioner that a letter containing the outcome of a patient complaint had been sent to the wrong address. The letter contained a complaint response and meeting notes from the investigation, which contained sensitive personal data relating to the patient. The error occurred as a digit in the address was accidently deleted when amendments were made to the letter and the address was not checked prior to it being sent. This incident follows several others of a similar nature. The Commissioner found that the temporary staff member who made the error had not received the appropriate training and guidance in relation to their role, there was a lack of formal checking procedures for correspondence, key recommendations following similar incidents had not been implemented, and there was a lack of senior managerial oversight. During the course of the investigation, the Trust notified the Commissioner of a further breach that a Birth Register could not be located, but was subsequently recovered.

Undertakings:

1. The Information Governance (IG) Committee should regularly review, test and oversee the achievement of IG training targets and staff awareness of IG issues.
2. Ensure that all staff in the Complaints team complete annual data protection training in addition to mandatory IG training, covering consent, confidentiality, security and records management.
3. Ensure that attendance at data protection training is monitored and there are procedures to ensure completion.
4. By 31 March 2016, submit a report to the Commissioner including a review of data flows, an information risk assessment of information assets and a detailed and updated Information Asset Register.
5. As soon as practicable, implement the approved option for legacy record disposal, monitor progress regularly and report outcomes at each IG Committee.
6. Create a procedural document for correspondence checking, which is signed by all relevant staff to show that they are aware of and understand the procedure.
7. Monitor the implementation of recommendations from data protection incident investigation reports, and make evidence of completion available to the relevant committees.
8. By 31 March 2015, provide evidence of the implementation of the above measures.
9. Implement such other measures as appropriate to ensure personal data is protected.

Findings of the ICO in relation to the undertakings signed:

N/A

International Trends

In the spotlight...

UAE

Overview

Recent developments in Europe spiked interest in data protection and security in the United Arab Emirates (UAE)[1]. The Court of Justice of the European Union's (CJEU) October ruling in Schrems v. Data Protection Commissioner (Case C-362/14), the decision which invalidated the legal basis for the transfer of personal data from the European Economic Area (EEA) to the USA under the Safe Harbor protocol, prompted UAE regulators and companies to examine their wider compliance with global standards.

UAE organisations with a footprint in the EEA are re-assessing the legal basis for transfers of personal data to the USA to third party organisations, cloud-based storage solutions and group companies. Certain regulators within the UAE have called on companies to re-assess data transfers made under the Safe Harbor protocol.

Regulatory landscape

Overarching legislation dealing solely with personal data protection and security does not exist in the UAE, but this does not mean UAE-based organisations can ignore this issue. The UAE Civil Code provides for a tort of misuse of private information. The Penal Code makes it a crime to publish or otherwise exploit personal information relating to an individual's private life.

There are several other laws issued at a Federal level containing data security elements. The financial, e-commerce and telecommunications sectors are regulated and must ensure data held by businesses in those industries is secured. Companies in the Dubai Healthcare City are subject to independent and European-style data protection regulatory framework.

The most commonly publicised data privacy-related fines in the UAE relate to the 2012 Cyber Crimes Law. Under this law, the unlawful invasion of privacy is a crime punishable with an US$ 136,000 (approx.) fine and/or incarceration. E-marketers can find themselves falling foul of this law if using personal information unlawfully. Towards the end of 2015, an individual who photographed and distributed the personal information of a famous footballer found himself in court for invasion of privacy.

Cyber security is a national priority in the UAE. Encouraged by a forward-thinking government, 2015 saw cyber security a buzzword in both the public and private sector. Many UAE businesses are seeing the commercial advantages of being 'cyber confident' and starting conversations with local experts. The UAE has a large online retail sector and e-commerce is continuing to rise in the region. The government is keen to ensure this is a safe business environment for consumers and has produced legislation to govern transactions.

The Dubai Health Authority has issued guidance for the secure retention and destruction of patients' health records based on international standards. The Authority wishes to move towards a greater dependency on online services for patient healthcare. The Health Authority of Abu Dhabi has also developed sophisticated regulatory requirements for handling and securing medical data.

Social media was also a hot topic in 2015. In the UAE, either corporate or individuals users of instant messaging services or social networks can be prosecuted for insulting other users or denouncing the State. A particular issue for large web-based operations is the obligation to keep websites clean of prohibited content, such as religious hatred, anti-establishment remarks and pornographic material.

Dubai International Financial Centre

Organisations with Dubai International Financial Centre (DIFC) operations are bound by a data protection law and regulator, the DIFC Data Protection Commissioner (DDPC), closely resembling the European operating model; so much so that the DDPC has followed the CJEU's Safe Harbor ruling. The DDPC recommended that DIFC organisations relying on the Safe Harbor protocol to legitimise the transfer of personal data to the US review the legal basis for the transfers.

1 - The UAE is a federation comprising of seven Emirates; Abu Dhabi, Ajman, Dubai, Fujairah, Ras Al Khaimah, Sharjah and Umm Al Quwain.

The DDPC conducts supervisory visits to DIFC organisations to observe compliance with the Data Protection Law and the Regulations. An organisation's data protection governance, structures, policies and procedures are scrutinised to ensure compliance with regulations. Data breaches must also be reported to the DDPC as soon as reasonably practicable.

According to the DDPC, the scope of the review for an entity is based on the relative size and complexity in processing personal data, the process of transferring personal data outside the DIFC and the security measures that they have in place to ensure an adequate level of protection for the data transferred, and that entity's record of transparency and co-operation with the DDPC.

More generally, the DDPC takes an active role in managing data protection in the DIFC. The Office recently published advisory guidance (law and regulations, notification process, amongst others) and takes regular enforcement action. The last major documented case of this was in 2013, when Fulcrum Capital was the subject of an enforcement notice for illegitimate processing of an employee's personal data.

Compliance obligations

There are limited instances of reported fines or sanctions for data protection and security issues in the UAE. This said, in 2015 there were some notable breaches across the energy, financial and technology sectors. In certain cases an obligation to report breaches to a relevant government ministry does exist, such as to the Health Authority of Abu Dhabi for medical data breaches.

Currently the DIFC is the only judicial system in the UAE to mandate filing notifications of personal data processing functions when companies intend on or begin to process personal data. As stated above, organisations within the DIFC may be the subject of a supervisory visit to monitor and assess compliance with the law. DIFC companies also need to lodge a request to transfer in the event that a data transfer outside of the DIFC is contemplated, the jurisdiction is not acceptable and none of the other exemptions apply to the transfer.

We expect the new Abu Dhabi Global Market, with a legal framework similar to that of the DIFC, to follow the DIFC in requiring companies to submit notifications for personal data processing functions.

Future developments

Regulatory reform resulting from the EU General Data Protection Regulation has prompted large organisations to review their internal policies to ready themselves for compliance, whether the organisation actually has or is first contemplating activities in Europe or involving EU citizens.

The UAE has constituted a government body, the National Electronic Security Authority (NESA), to protect the UAE's critical infrastructure. More generally, NESA's functions are to promote cyber security best practice in the UAE by drawing on internationally recognised standards.

Waseem Khokhar
+9714 304 3181
Waseem.khokhar@pwclegal.co.ae

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

Bassim Ousta
+9714 304 3983
Bassim.ousta@pwclegal.co.ae

Australia

Privacy issues in Australia have, since 2010, been administered by the Office of the Australian Information Commissioner (OAIC). However, in May 2014, the Australian Government announced an intention to disband the OAIC and move these functions to a new Office of the Australian Privacy Commissioner. The Bill to implement these changes was passed by the House of Representatives but the Bill has not yet to be considered by the Senate. This has created some confusion as to the ongoing functioning of the OAIC. In January 2016, the Acting Privacy Commissioner's term was extended by the Attorney General through to April 2016 with a further extension now likely.

2015 OAIC activity

Notwithstanding the uncertainty surrounding the future of the OAIC, 2015 has seen a marked increase in the OAIC's level of activity. In 2015, the Office:

- Handled 12,241 privacy enquiries;
- Received 2,838 complaints, successfully closing 1,976;
- Managed 117 voluntary data breach notifications;
- Undertook 12 privacy assessments (formerly known as audits), involving 85 entities, to assist compliance with good personal information handling practices and making recommendations to improve privacy practice;
- Issued 32 sets of guidance material to assist entities covered by the Privacy Act; and
- Increased the number of matters considered by the commissioner under the section 52 determination powers of the Privacy Act.

First enforceable undertaking – Singtel Optus

In March 2015, using new powers introduced into the Privacy Act in 2014, the Commissioner accepted an enforceable undertaking offered by Optus, a major Australian telecommunications company, following three significant privacy incidents where the security of personal information held by Optus was compromised.

An enforceable undertaking is an agreement between the OAIC and an organisation or agency that creates a binding commitment to take steps to ensure privacy compliance. An enforceable undertaking can be enforced by the Commissioner in the Federal Court. In its undertaking, Optus agreed to complete a wide ranging independent review of its information security systems and to implement any recommendations resulting from this review.

Metadata – Ben Grubb v Telstra Corporation Limited

In May 2015 the Privacy Commissioner found Telstra, another major Australian telecommunications company, had breached an individual's privacy, Mr Grubb, by failing to provide him with personal information about him held by Telstra, specifically the topical issue of anonymous metadata. The Commissioner agreed with Telstra's argument that much of the metadata sought was not 'personal information' because on its face the data was anonymous. However, the Commissioner found that this overlooked the reality of data-linking and that a customer's identity and other information about them can be established by cross-matching data sets, thus constituting personal information.

The Commissioner found that personal information is not just that which does identify an individual but also that which reasonably can. The case provides guidance on the potential risks faced by companies handling complex data sets to which anonymous data can be linked. The Commissioner particularly highlighted retailers and loyalty programs as having exposure to this risk.

Mandatory breach notification

The Australian Government has proposed a mandatory data breach notification scheme that would require agencies and organisations to notify individuals in the event of a serious breach of security if it leads to the disclosure of personal information. The Government has issued a public consultation on the form of the amendment and is seeking submissions by 4 March 2016. The proposed scheme would be in line with other jurisdictions (USA, EU and OECD guidelines) that currently have a mandatory breach notification scheme. Some distinctive features of the Australian scheme, as it is now drafted, include:

- A relatively higher notification threshold, only in serious cases;
- A simpler single-tier scheme for notification to both the regulator and affected individuals; and
- Flexibility for cases involving adequately encrypted information as it poses less risk of harm to affected individuals.

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

Yolanda Chorazyczewski
+61 (2) 8266 2471
Yolanda.chora@au.pwc.com

Belgium

Data protection landscape is taking shape in Belgium

Data protection, privacy and digital issues benefit from a prominent position on the political, judicial and regulatory agenda in Belgium.

2014 marked the year in which Belgium appointed the first EU State Secretary for Privacy and the beginning of an era of change in the Belgian privacy landscape. 2015 followed with the first results: the GDPR negotiations came to a close, a Belgian landmark court case was decided and important legislative changes have been announced.

The Belgian Regulator

The Belgian Privacy Commission (the Commission), officially named the "Commission for the Protection of Privacy" is the Belgian Data Protection Authority.

In contrast to the DPA's in Belgium's neighbouring countries, the Commission has fewer tools or means available to ensure effective enforcement and was, until recently, considered to be less active, or at least not so much in the forefront, towards non-compliant organisations. In 2015, this perception has changed, mainly following past actions taken against a number of important social media providers and the Commission's visible responses to the privacy hurdles of today's digital age. They have clearly shifted to a more active stance.

2014 report, published in 2015

The Commission reports on its acti

there was a small decrease in the number of complaints filed with the Commission (413) in comparison with 2013 (450). Most complaints related to privacy principles (20%), economic matters (18%), processing of images (19%), market practices (12%), and telecom matters (8%).

There was, however, a significant increase in Belgian organisations notifying their data processing activities with 38% more notifications than in 2013. This is likely to relate to a greater awareness of data protection regulation and a commitment to be compliant in Belgium, in addition to more organisations processing personal data. Note that this obligation will soon disappear when the new GDPR will come into force.

The annual report also highlights some key events of 2014 including the GPEN Privacy Sweep Day (reviewing the privacy compliance of mobile apps) and the introduction of the joint web-tool of the Belgian Telecom Regulator (BPIT) and the Commission, which is used for data breach notifications by telecom providers (as mandatory under ePrivacy Regulations). In 2014 we saw 3 mandatory and 15 voluntary data breach notifications.

2015 report, to be published in 2016

The 2015 annual report is expected to be released towards the end of spring 2016, and we anticipate that it will highlight an increase in the number of interventions of the Commission, especially in view of the GDPR as well as in light of the higher level of scrutiny of the Privacy Commission with respect to cross-border transfers of personal data to the USA and other non-EU countries (following the CJEU Schrems Case on Safe Harbour and the announced Privacy Shield).

General Data Protection Regulation

In December 2015, the Belgian Secretary for Privacy announced that he will not wait until the General Data Protection legislation becomes applicable but will immediately start to amend the Belgian Privacy legislation.

We expect the first changes will relate to the previously announced introduction of new powers and tasks for the Privacy Commission which will transform it from an advising body to a proactive one that can impose monetary fines and take direct enforcement actions, e.g. blocking access to the databases of companies who do not act in compliance with the law.

Court cases

In the past, active enforcement actions were rare in Belgium. This seems to have changed, with the Belgian Data Protection Authorities picking up the pace alongside their counterparts in other EU countries and following landmark EU court cases in data protection.

A clear example is the decision of 9 November 2015 of the President of the Brussels Court of First Instance which ruled in favour of the President of the Belgian Privacy Commission, and ordered a key social media provider to cease tracking non-users and stop storing personal data, with the risk of a fixed fine of EUR 250,000 per day until compliant.

What to expect for Belgium in 2016?

Aside from the privacy challenges which Belgium is currently facing in the fight against terrorism, we expect the major challenge for businesses and other data-stakeholders in 2016 to relate to the implementation of the GDPR. We already see many organisations taking proactive steps to start mapping their data flows and assessing the impact of the GDPR and the road towards compliance.

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

Canada

Canada's Anti-Spam Law ("CASL")

In 2015, the Canadian Radio-television and Telecommunications Commission ("CRTC") was active in handing out sanctions for CASL violations.

Porter Airlines Inc. ("Porter") agreed to pay $150,000 for sending emails in violation of CASL's commercial electronic messages ("CEM") rules between July 2014 and April 2015. During its investigation, the CRTC discovered that Porter did not have proof of consent, some messages did not provide complete contact details and other messages contained non-functioning unsubscribe links. As part of the undertaking, Porter agreed to update and implement its compliance program to ensure corporate compliance policies and procedures, training and education, monitoring, auditing and reporting mechanisms. Porter also agreed to comply with, and ensure that any third party authorized to send CEMs on its behalf complies with the regulations.

Rogers Media Inc. ("Rogers") agreed to pay $200,000 for sending emails in violation of CASL's CEM rules between July 2014 and July 2015. Rogers sent CEMS with an unsubscribe mechanism that did not work or could not be used by the recipient, failed to honor unsubscribe requests within 10 business days and the electronic address sent in CEMs to unsubscribe was not valid for the required 60 days following the sent message. As part of the undertaking, Rogers agreed to update and implement its existing compliance program, which includes reviewing its written policies, developing training programs, and registering and tracking all complaints related to CEMs and their resolution.

Compu-Finder received a $1.1m penalty for sending emails in violation of CASL's CEM rules between July and September of 2014. Compu-Finder sent CEMs without the recipients' consent and without functional unsubscribe mechanisms.

Legislation evolution

In January of 2015, phase 2 of CASL that focuses on the installation of computer programs came into force. Phase 2 applies to the installation, or the causing of installation of software, on someone's computer without consent. However it does not apply to owners or authorized users installing software on their own computer systems. Failure to comply can result in monetary penalties of up to $10,000,000 for organizations and $1,000,000 for individuals.

In healthcare, Ontario is making an effort to improve privacy and accountability by introducing new measures to protect personal health information of patients. The Health Information Protection Act of 2015 ("Act") would make breach reporting mandatory, increase transparency and double fines for offences to $100,000 for individuals and $500,000 for organizations. These amendments have been introduced in order to help combat employee snooping of patient files. The Act was introduced on September 16, 2015 and it is in second reading as of December 10, 2015.

Effective June 18, 2015, the Digital Privacy Act amended PIPEDA by specifying that in order for consent to be valid, individuals must understand the nature, purpose and consequences of data processing to which they are consenting. Other changes include exceptions when personal information can be collected, used and or disclosed without consent, such as in business transactions, in witness statements in insurance claims, in identifying injured, ill or deceased individuals or in situations of financial abuse. In addition, the Privacy Commissioner can now enter into compliance agreements with organizations to ensure compliance with PIPEDA.

PIPEDA amendments that still need to be finalized include mandatory breach reporting. Once the breach notification is in force, organization will be required to notify the Office of the Privacy Commissioner of Canada ("OPC"), affected individuals and relevant third parties about breaches of security safeguards that pose a "real risk of significant harm" to affected individuals. Factors that organizations will need to consider when assessing the presence of a real risk of significant harm include the sensitivity of the information involved and probability that the

information was or will be misused (or any other prescribed factor). Organizations that knowingly fail to report to the OPC or notify affected individuals of a breach that poses a real risk of significant harm, or knowingly fail to maintain a record of all breaches can face fines of up to $100,000. Organizations will also be required to keep and maintain a record of every breach of security safeguards involving personal information under their control.

Outlook for 2016

In 2016 we will continue to see a rise of the Internet of Things ("IoT") and wearable technology. IoT enables multiple devices to connect to the Internet, interact and interoperate, therefore making people's lives more efficient. However, these devices collect a vast amount of personal information that could easily create user profiles and subject individuals to potential harm. Organizations must ensure that adequate data governance programs and safeguards are in place in order to protect personal information and uphold consumer trust.

The CRTC will continue to promote compliance with CASL by enhancing intelligence and taking enforcement actions. Organizations should audit current practices and consents and develop corporate compliance programs that can support their claim of due diligence to avoid any enforcement notices or monetary penalties.

Canada's majority Liberal government that was elected in 2015 has committed to ensuring an open and transparent government. The Liberal government will implement initiatives that expand Canada's access to information, which applies to the Prime Minister's and Ministers' Offices, as well as that administrative institutions that support Parliament and the courts. An all-party national security oversight committee will be created in order to monitor and oversee the operations of every government department and agency with national security responsibilities.

Bill C-51 (the Anti-Terrorism Act of 2015) is now law. This is a controversial Act that broadens that authority of Canadian government agencies to share information about individual. The Liberal government is now being pushed to continue its support of the repeal of the problematic elements of this Act and to introduce legislation that can both improve security of Canadians while protecting rights and freedoms. Government surveillance is also a key point of focus for the OPC and it is issuing recommendations for potential improvements to legislation to protect both national security and privacy.

The OPC will focus on 'Reputational Privacy' by creating an environment where individuals are free to use the Internet without fear of a digital trace that could lead to an unfair treatment. Vulnerable groups, including senior citizens and youth will be a primary point of focus. In addition, the OPC will issue a 'Right to be Forgotten' paper for consultation and develop a policy position in Canadian legal context.

Another point of focus for OPC will be in the area of 'Government Surveillance' and the implementation of national security legislation. Specifically, the area of interest includes Bill C-51, the Anti-Terrorism Act of 2015 and examining the collection, use and sharing practices of departments and agencies involved in surveillance activities to ensure that they comply with the Privacy Act.

Jordan Prokopy
+1 416 869 2384
Jordan.prokopy@ca.pwc.com

David Craig
+1 416 814 5812
David.craig@ca.pwc.com

China

Draft Cybersecurity Law

On 8 July 2015, the Standing Committee of the National People's Congress, which is the legislative body of China, released the Cybersecurity Law of the People's Republic of China (Draft) for public consultation. It demonstrated China's determination to take a more effective and coordinated approach to safeguard the cyberspace as part of China's National Security Initiati

tors and network service providers who use networks owned or administered by others in order to provide relevant services. This includes, but is not limited to, telecommunication operators, network information service providers, and important information system operators.

In addition, "critical information infrastructure operators", which includes critical industries such as public communication, media, energy, transportation, financial services, public utilities, medical, social welfare, military and government affairs as well as network service providers with a significant number of users, are subject to stringent requirements under the proposed law.

Key challenges

Network operators have increased obligations such as censorship duties to prevent the spread of prohibited and illicit information and they are subject to more regulatory scrutiny. Violations may result in punishment including warnings, fines (on both the business and responsible supervisor(s)) and suspension of business.

The scope of "critical information infrastructure operators" is broad and they are subject to a set of detailed requirements such as storing "personal and important information" within the territory of China, performing a "security evaluation" in accordance with requirements set out by the relevant authorities (which are yet to be published) prior to any cross-border transfer of such data for legitimate business reasons, passing security examinations for purchasing network products and setting up internal security roles and responsibilities.

Key network equipment, products and services must be accredited by qualified institutions before they can be sold.

The Chinese government has the legal power to shut down or limit network communications under the proposed law to maintain social stability in case of significant social security emergencies (e.g., previously deployed during the Xinjiang Uygur riot in 2009), which may impact an organisation's business operation, and hence, its business continuity considerations.

It is estimated that the draft law will be formally adopted in early 2016. However, as it is high level in many aspects, it is unclear as to how it may be enforced. Government agencies will issue additional industry specific guidelines, resulting in more detailed requirements being published.

More Severe Punishment for Crimes Related to Personal Information

On 29 August 2015, the Standing Committee of the National People's Congress passed the 9th Amendment to the Criminal Law of China, which became effective on 1 November 2015.

Under this Amendment, penalties have increased from three years to 3-7 years of imprisonment for the crime of selling and illegally providing personal information of citizens and for illegally obtaining personal information of citizens. The two acts have only been criminalized in China since 2009 and such increased penalties demonstrate that the Chinese authorities want to strengthen personal information protection for individual citizens.

Jenny Zhong
+86 (0)10 65 33 29 08
jenny.j.zhong@cn.pwclegal.com

France

Safe Harbor

Following the invalidation of Safe Harbor, on 19 November 2015, the CNIL (French Data Protection Authority) took an official position in line with other European data protection authorities, regarding transfers of personal data from France to the U.S. using the Safe Harbor scheme.

The CNIL confirmed that transfers of personal data towards the US using the Safe Harbor scheme were now illegal in France. As a result, data controllers subject to French law must amend their existing notifications by either declaring that their data transfers to the U.S. have ceased, or indicating that the data transfers will be based on another data transfer mechanism (in practice Binding Corporate Rules ("BCRs") or EU Standard Clauses). However, the CNIL also specified that the impact of the CJEU ruling on BCRs and EU Model Clauses is still being discussed between the G29 members and therefore, reliance on such transfer mechanisms remain temporary solutions. Indeed, in the absence of any new legal framework adopted by EU institutions and Member States, the European Data Protection Authorities have already decided to discuss the possibility to use their enforcement prerogatives to suspend or forbid data transfers to the U.S.

Formal notices

CNIL orders Google to apply delisting on all Google domain names

Since the European Court of Justice ruling of 13 may 2014 which recognized the right to delisting, a EU individual may request search engine companies to remove search results displayed following a search based on a personal name. To this date, Google received tens of thousands of requests from French citizens, but only proceeded to delist some results, based on some Google geographical domain name extensions (.fr; .es; .co.uk; etc.). Such delisting was not applied to other Google geographical extensions (i.e. the ones not concerned by the delisting request) or generic extensions (such as on google.com), which any internet user may visit alternatively.

In May 2015, the President of the CNIL sent Google a formal notice to proceed with the delisting on all of Google's domain name extensions. At the end of July, Google filed an appeal in order to obtain the withdrawal of this public formal notice, arguing that such formal notice constitutes a violation of the public's information right. The CNIL rejected this appeal, notably on the ground that limiting the delisting to geographical extensions could be easily circumvented in order to find the delisted result; it would be sufficient to perform the search on another extension, and notably on the generic one "google.com".

Dating websites put on notice to comply with French Data Protection law

In 2015, eight French companies operating dating sites (including Adoptaguy, Meetic and Toodate) were put on notice by the CNIL to take actions in order to comply with the French Data Protection Act. The CNIL considered that these companies (i) did not delete profiles of users who have explicitly requested that their account be removed and/or (ii) did not provide sufficient guarantee regarding security of the data processing. Most importantly, the CNIL considered that the websites did not obtain prior consent of the users when collecting "sensitive data," including ethnicity, political opinions and health-related data.

Financial sanctions

The CNIL is entitled to 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.

In 2015, the main sanctions applied by the CNIL were the following:

- 5 November 2015: €50,000 fine against the French company Optical Center

for a breach of its obligation regarding customers 'data confidentiality and privacy.

- 1 June 2015: €15,000 fine against the French company Prisma Media for sending information letters without prior consent of data subjects.

Court Decisions

On 8 September 2015, the French Cour de Cassation ruled that any personal data processing should be subject to prior formalities with the CNIL, even where such processing only concerns one single data subject and where few data is processed. Criminal penalties may apply for failing to do so, namely five years' imprisonment and a fine of up to €300,000 (€1,500,000 in case of a company).

On 23 March 2015, the French Conseil d'Etat confirmed CNIL's sanction, a €10,000 fine, against a company operating a French case law database after the company did not comply with the CNIL's formal notice to proceed with the anonymisation of individuals' names.

Practices and Recommendations of the French data protection authority (CNIL)

Binding Corporate Rules (BCRs) - simplified formalities

Since 2015, the CNIL now delivers single decisions (autorisations uniques) which simplify data controllers' formalities regarding data transfer outside the European Union. Hence, group entities subject to compliance with the French Data Protection Act will no longer have to apply for each transfer outside of the European Union to be granted an authorisation.

Children's privacy - CNIL reminds websites owners of their obligations

Alongside 29 other national data protection authorities, the CNIL has been part of the "Internet Sweep Day" which notably performs audits regarding children's privacy in respect of child and teenager oriented websites.

The CNIL identified several breaches to legal requirements such as lack of information of internet users. In particular, the CNIL stated that many websites did not implement any monitoring measures and that parental consent remained rarely requested.

Information letters have been sent to French websites requesting them to comply with the French Data Protection Act. Failing to do so, the CNIL may implement its specific sanctions procedures.

Cookies - situational analysis after the CNIL

IL's 2013 recommendation to professionals specifying how to comply with legal requirements regarding the use of cookies, the CNIL proceeded with 24 on-site investigations, 27 on-line investigations and 2 hearings. Two years after its recommendation, the CNIL identified that many websites were still using cookies without the prior consent of users (notably by means of a header on the front page).

In a press release dated 30 June 2015, the CNIL disclosed that it had sent more than 20 formal notices to infringing websites so far.

Sophie Delahaie-Roth
+33 3 90 40 26 10
sophie.delahaie-roth@pwcavocats.com

Michael Chan
+ 33 3 90 40 26 13
michael.chan@pwcavocats.com

Germany

Notwithstanding sector-specific legislation, data protection in Germany is mainly regulated in the private sector by the Federal Data Protection Act (Bundesdatenschutzgesetz) (BDSG), which implements the Data Protection Directive 95/46/EC.

The data protection authorities of the states (Länder) are competent for the enforcement. In general, they do not publish the enforcement acti ties, unless they are matters of public interest.

Reports

Approximately every two years, however, they issue a report of their activities. The different reports show that only around 55% of the German Federal States have given a detailed insight into their sanction proceedings. Although the amount of penalties is on average comparably low, there is a tendency towards stricter sanctions. For example, the State of Thuringia noted that "the number of cases from 2011 to 2012 have increased by 100%, and from 2012 to 2013, by 250%. The trend is still rising."

All reports provided by the German Federal States stressed that imposing fines and the related proceedings caused more effort compared to the last years, thus more manpower and financial resources must be made available to satisfy the constantly increasing demands on process control.

Notable sanctions

The Hamburg Data Protection Authority fined a tech company €145,000 for collecting data from unsecured Wi-Fi networks over a period of three years.

In another published case, the North-Rhine-Westphalian Data Protection Authority fined an operator of gas stations who carried out extensive video surveillance of customers and employees on the premises and service areas. Video recordings of some branches of the company were also available on the Internet by entering the respective web-address. The operator was fined €54,000.

The published sanctions are specified in more detail in the table below.

Outlook

We expect that the tendency towards more and stricter sanctions will continue.

Federal state	*Number of offences in the annual report*	*Total fines (in €)*	*Other*
Baden-Wuerttemberg	Not specified	Not specified	Two cases have been referred, a fine was not imposed.
Bavaria	Not specified	Not specified	The report only addressed the cases in which a fine will be imposed.
Berlin	25	88,205	-
Brandenburg	19	10,300	-
Bremen	> 4	Not specified	Four cases were mentioned as an example, but there is no information about the total number.
Hamburg	12	218,466	€145.000 fine to Google Inc..
Hesse	20	1,750	20 fine proceedings, but 18 were terminated. Just in 2 cases a fine was imposed.
Mecklenburg-Western Pomerania	1	Five-digit	-
Lower Saxony	41	Not specified	-
North Rhine-W tphalia	4	64,000 +	1. €64,000 fine imposed 2. Very high fine imposed 3.+4. No action specified
Rhineland-Palatinate	12	Five-digit	-
Saarland	29	Not specified	-
Saxony	95	17,485	-
Saxony-Anhalt	Not specified	Not specified	The report only addressed the cases in which a fine will be imposed.
Schleswig-Holstein	2	18,000	-
Thuringia	Not specified	Not specified	The number of cases increased from 2011 to 2012 by 100% and from 2012 to 2013 by as much as 250%. The trend is still rising.

J

-peter.ohrtmann@de.pwc.com

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

India

India has not yet implemented an overarching data protection law. However, the Information Technology Act (2000) (IT Act) has been amended to include section 43A and section 72A which give a right to compensation for improper disclosure of personal information. The associated Rules impose additional data protection requirements on commercial and business entities regarding the collection and disclosure of sensitive personal data or information.

Under the Rules, sensitive personal data or information means information which relates to:

1. Passwords;
2. Financial information such as bank account or payment card details;
3. Physical, physiological, and mental health conditions;
4. Sexual orientation;
5. Medical records and history;
6. Biometric information;
7. Any details related to the above information, as provided to a body corporate for providing services; and
8. Any of the information received under the above clauses by a body corporate for processing, which is stored or processed under lawful contract or otherwise.

Upcoming 'right to privacy' law

India is in the process of enacting a specific right to privacy law which it has been working on for some years now, having released the first draft in 2011. The law seeks to protect individuals against breaches of their privacy through unlawful means.

Launch of the Certified Privacy Professional (DCPP) Program

The Data Security Council has launched a certification program for aspiring privacy professionals, which it hopes will help to develop a stronger privacy workforce in the country. The program will teach general privacy concepts and provide updates on the current privacy landscape, both in India and major economies further afield. The program is open to those working in both industry and government sectors.

Activity in privacy in 2015

- In May, one of India's most popular music streaming services, Gaana.com, suffered a hack of their website which resulted in millions of user's information being exposed publically. It is not known whether the suspected hacker will face prosecution, however under the IT Act, those that commit hacking are liable to imprisonment for up to three years and a fine of up to approx. $3,000 USD.
- In September, a woman was arrested for hacking into a destroying data on her ex-employers company computers. The company lodged a complaint against her under the IT Act and the police are investigating, which has involved her arrest and the seizure of computer equipment.
- In late 2015, following a cyber attack in the UK, a telecommunications company faced a further breach of customer personal data due to scam calls being made from its Indian call centre. As a result, three people have been arrested and the company is reviewing its relationship with the call centre provider, Wipro.

Rajinder Singh
+91 9873264886
rajinder.singh@in.pwc.com

Italy

This is a short overview of the enforcement actions taken by the Italian Data Protection Authority (IDPA) in 2015.

The IDPA's online database (www.garanteprivacy.it) reveals the key areas which the authority focused its attention on during 2015: marketing-related data protection issues (with specific reference to the processing of personal data and their disclosure to third parties without the previous consent of data subjects), absence of information notices (amongst others, in connection with video surveillance systems), disclosure of sensitive data to the public and the right to be forgotten.

Each June, the IDPA issues its Annual Report containing the summary of the activities performed and the decisions taken in the previous year. Therefore, June 2016 will be an important milestone to analyze enforcement trends in 2015.

Marketing-related data protection issues

The most significant financial penalties inflicted during 2015 by the IDPA pertains to marketing-related data protection issues.

Amongst others:

The IDPA imposed a fine of €200,000 to a leading Italian electric energy supplier. The entity processed personal data for marketing purposes without a proper information notice and without obtaining prior explicit consent from the data subjects.

The IDPA imposed a fine of €130,000 to a large telephone company for publishing the mobile phone numbers of 35 individuals in the public phone book, without obtaining their prior consent.

Absence of information notices to data subjects

An individual who owned several websites created a database containing about 300,000 e-mail addresses of registered data subjects and later transferred this database to a marketing company.

According to the IDPA investigation, information notices were not made available to the data subjects on the website registration page and the individuals were not put in a position to give specific consent for the processing of their data for marketing purposes, nor for their transfer to third parties. In light of the above, the IDPA inflicted a fine of €64,000 to the individual who created the database.

A fine of €32,000 was issued to an Italian bank who did not provide two clients with an information notice when opening their bank accounts, nor obtain any consent for the processing of their personal data.

The IDPA issued a fine of €16,800 to a company which failed to provide its customers with an information notice on a website registration page. The fine also took into account that the company had a video surveillance system in place and (i) the information notice submitted to the employees gave no indication of the data controller nor the purpose of the video surveillance system and (ii) the images gathered from the surveillance system were kept by the company for longer than permitted by law.

Disclosure of sensitive data to the public

Another significant case examined by the IDPA related to the publication of sensitive personal data on the website managed by the Health Department of an Italian Region– namely, information that could reveal the health status of individuals. The Department published lists of job positions reserved, by law, to individuals suffering disabilities, together with the details of the relevant assignees (including their name, surname and date of birth).

The IDPA declared this disclosure unlawful and directed the Region to stop this publication immediately and to comply with the guidelines set forth by the IDPA in the future.

Right to be forgotten

As envisaged in 2014, Google Spain's case had a significant impact on Italian data protection this year.

The IDPA decided on about 50 claims filed by individuals, public entities and professionals, requesting Google Inc. and/or Google Italy S.r.l. to remove certain links from the list of results available through the search engine.

The IDPA accepted about 1/3 of claims and directed Google to remove the links, due to the absence of any public interest justifying their availability. In the other cases, the IDPA considered that the public interest in obtaining the information prevailed. Indeed, such cases mainly related to recent judicial proceedings, which were held to be relevant and in the public interest, given that the majority of the proceedings remained ongoing at the date of the claims. Additionally, most cases only disclosed minimal data of the subjects involved, thus respecting the "minimalisation of information" principle.

Stefano Cancarini
+39 02 91605212
Stefano.cancarini@it.pwc.com

Filippo Riva
+39 02 91605224
Filippo.riva@it.pwc.com

J

Two key developments in 2015 were the revision of the "Act on the Protection of Personal Information" and the introduction of the "Act on the Use of Numbers to Identify a Specific Individual in the Administrative Procedure" (the so-called "My Number Act"). The My Number Act introduced a unique identification number for all residents of Japan, for social security and taxation purposes, which is defined as Personally Identifiable Information (PII). Throughout 2015, many Japanese companies dedicated significant time and resources to prepare for the introduction of the My Number system and will continue to do so throughout 2016 and beyond.

In addition to the legislative developments, Japan has witnessed several high-profile privacy breaches. Perhaps the most notable example being the huge information leakage by the Japan Pension Fund in 2015 of some 1.25 million personal information records, leading to widespread concerns of the Japanese authorities' ability to protect personal information held under the My Number system.

Global business trends which impact privacy are also being reflected in Japan. For example, the use of Big Data in corporate Japan is growing, in addition to the inherent challenges in protecting personal information which it entails.

Revision of the Act on the Protection of Personal Information

Japan first established specific legislation on personal information protection in 2005 with the enactment of the "Act on the Protection of Personal Information". This law defined appropriate handling of personal information, in addition to security requirements.

10 years have passed since its enactment and many factors such as data proliferation, significant and high-profile personal information leakage incidents and the establishment of the My Number Act have led to the requirement for more robust legislation, with the resultant revision of the Act on the Protection of Personal Information coming in September 2015. This revision includes clearer definitions of personal information and addresses previously ambiguous issues such as cross-border and third-party data sharing, particularly with regard to anonymised data. Additionally, the revision saw the creation of the Personal Information Protection Committee established to oversee and enforce the revised act, although how active this committee will be remains to be seen.

My Number Act

The controversial My Number Act was established in 2015 September. "My Number" is a 12 digit individual number used for government administrative purposes. Companies need to handle My Number records when preparing and submitting legal records relating to their employees to authorities for most administrative purposes, as My Number must be printed on such records.

Companies are required to implement stringent security management systems in the administrative processes where My Number records are handled because its unintended use or leakage would represent a leakage of "Specific Personal Information", to which specific security requirements are mandated in the My Number Act and relevant guidelines.

Handling My Number records requires companies to notify the individual of the purpose of its use, implement high-level security arrangements when storing the data, perform outsourcing management if a company outsources the handling My Number to third party, and to dispose of the data related in a timely manner when no longer relevant.

A My Number record is also given to all registered legal entities. This is made available on the National Tax Agency's web site, where legal entity My Number records can be freely viewed and downloaded. Companies can utilise the My Number of registered legal entities free of the security management requirements which are applicable to individuals' My Number records.

Prior to the introduction of the My Number system, many companies prepared by taking measures such as identifying their My Number handling processes and relevant legal records, data identification processes, and customising the internal controls on their IT systems (such as their HR or accounting system). In addition to this, many companies revised their policies, guidelines, operation procedures and training programmes for their employees to ensure appropriate handling of My Number data. Because of the potential scale of impact of the My Number introduction, however, many small to mid-size companies have struggled to be appropriately prepared in time.

Concerns linger around the long-term feasibility of the My Number system. Prior to the commencement of the My Number system, My Number notification cards were delivered to all residents in Japan, but around 10% could not be delivered at the end of 2015 because of the absence of recipients or incorrect residential addresses. The Japanese government has also conducted widespread awareness campaigns regarding the My Number system over the past year, but the general public still lacks sufficient understanding of and enthusiasm for the My Number system.

Assuming a successful roll-out, one potential further development is to link individual My Number's to each resident's bank account to allow government identification of issues such as benefit fraud. There is currently a three year grace period until this is implemented on a voluntary basis, with mandatory linking of My Number and bank accounts expected around 2021. The utilisation of My Number in various other areas is still under discussion, with one such possibility being health records.

Kenichi Kotaki
+81 (0)80 3445 2028
kenichi.kotaki@jp.pwc.com

Paul Graham
+81 (0) 80 4937 6267
paul.p.graham@jp.pwc.com

M

The Mexican data protection authority, which has recently changed its name to the National Institute for Transparency, Access to Information and Protection of Personal Data (IN I), does not publish enforcement cases - a key indicator 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, including guidelines regarding "Privacy Notices" and "Self-Regulatory Schemes".

Data Protection rose to prominence 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 what is now the INAI as the Mexican Data Protection Authority.

Following this, the Federal Law on the Protection of Personal Data held by Private Parties (the Law), entered into forced 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 INAI has the power to issue fines from 100 to 320,000 days of the Minimum Wage in Mexico City. Where a breach includes processing sensitive personal data, the sanctions may be doubled.

The INAI will base enforcement 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 authorised 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 authorised to transmit such data.

Enforcement Actions (2015 examples)

- **Resolution:** A private security company was condemned by the INAI for failing to answer a Subject Access request and to provide the data subject with a copy of the personal data held in its database and a copy of its privacy notice. Failure to do so within 10 days of the resolution results in a liability to fine.
- **Fine:** A secondary school was fined approx. $22,000 USD after the INAI received a complaint that the school published personal data of children online without their parent’s consent. The processing was not compliant with the purposes set out in the privacy notice and the school failed to provide information to the INAI upon formal request.

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

New Zealand

New Zealand Privacy legislation is more than 20 years old (Privacy Act 1993), and while there have been some amendments over time, it is not comprehensively equipped to govern and regulate privacy in a rapidly changing digital landscape. Recognising this, privacy law reform was signalled by the Minister of Justice in 2014, although there is yet to be a bill before Parliament. The Act defines 12 privacy principles, which should guide the use of personal information. The act does not require notifications to individuals in the event of a breach and as a result we ty thing" and notifying the affected individuals in the event of a breach.

In terms of punitive arrangements, the Privacy Act does not provide enforcement powers to the Privacy Commissioner. As a result, cases that relate to breaches of privacy in New Zealand are usually brought under human rights legislation (Human Rights Act 1993), where no mutually agreeable resolution can be found.

Below is an overview of key decisions and activities of the Office of the Privacy Commissioner (OPC) in 2015.

Immigration New Zealand (INZ) refuses to correct birth date

In 2011, an individual from Ethiopia, who had been orphaned at a very young age, came to New Zealand as a refugee sponsored by his aunt. Birth registration was not compulsory in Ethiopia when he was born, so there were no records of his date of birth. His aunt consulted with locals and estimated that he was born in early 2000. She used this date to apply for an Ethiopian passport and birth certificate on his behalf. She then used these documents to support his refugee application.

Subsequent investigations and medical examinations which indicated that he was likely to be at least 3 years older and in 2013, he asked INZ to change his birth year to 1996 based on this information. INZ refused. The incorrect birth date restricted the man from accessing a number of entitlements he should have been eligible for – such as a driver's licence and financial assistance for studying.

In this case, The Privacy Commissioner believed the complainant's case had merit and that there is a need for a legal precedent to help guide similar cases in the future. The Commissioner has therefore referred the matter to the Director of Human Rights Proceedings.

Government agency accidentally discloses informant's identity to employer after workplace complaint

A woman made complaints about the work practices of her employer to a government agency and she asked the agency to ensure that her details remained confidential.

The agency sent an inspector to visit the woman's workplace to investigate the complaints. The inspector showed the employer his notes, which had not been edited to remove the woman's name. In doing so, the inspector accidentally disclosed the woman's name to the employer. The woman said the disclosure of her name and the nature of her complaints led to the complete breakdown of the employment relationship. She said she was abused and humiliated by her employer.

The woman complained to the Privacy Commissioner that the agency had disclosed her personal information (her name) to her employer. The agency met with the woman and apologised. The agency said the inspector made a mistake when he showed the employer his notes, and explained the steps it had taken to ensure the situation did not occur again. The agency acknowledged it had breached principle 11 of the Privacy Act.

The agency offered to pay the woman's legal fees and some compensation in recognition of the fact that she lost her job, which the woman accepted.

Woman awarded $168,000 as a result of privacy breach

Human Rights Review Tribunal (HRRT) found that NZ Credit Union Baywide, had seriously breached privacy principle 11 by disclosing an ex-employee's private Facebook photo to recruitment agencies and her new employer.

The woman who iced a cake with derogatory comments about her former employer, has won her claim that her privacy was breached when the company took an image of the cake from her Facebook page – which was posted privately to her friends - and used it to harm her employment opportunities.

The HRRT ordered NZ Credit Union Baywide to pay a record $168,070 in damages to the woman and apologise to her "for the severe humiliation, severe loss of dignity and severe injury to feelings".

The company must also retract information it sent to staff and other agencies about her, and undertake training to ensure all staff understand the Privacy Act.

Andrew Parker
+64 4 462 7104
drew.x.parker@nz.pwc.com

The Netherlands

Increased fines

As a result of the recent bill on Data Breach Notifications, from 1 January 2016 the Dutch Data Protection Authority (DPA), which is operating under a new name of 'Autoriteit Persoonsgegevens' as per 1 January 2016, has the power to impose highly increased sanctions.

Penalties have been categorised based on the nature and severity of each violation. There are also guidelines which set out aggravating and mitigating circumstances for determining the level of the penalty which may ultimately be applied by the Dutch Data Protection Authority in specific cases. The maximum penalty per violation has been increased from EUR 4,500 to a maximum amount of EUR 820,000, or 10% of the company's annual net turnover, per violation. The fine may not only be limited to the Dutch establishment but could also include global group revenues.

New data breach notification requirement

The new bill introduces an obligation to report security infringements to the Dutch DPA immediately. The obligation to notify the Dutch DPA will exist if the infringement has, or is likely to have, serious adverse consequences for the protection of personal data. The Dutch DPA has issued guidelines to assist enterprises in deciding whether to report a data breach. The decision will involve an assessment based on an interpretation of all relevant facts and circumstances to determine whether an obligation to report a data breach exists. Companies experiencing a data breach will be responsible for this assessment, which makes it necessary for IT security, legal and compliance departments to work closely together.

The notification to the Dutch DPA must include a description of the nature of the breach and where additional information on the breach may be obtained. It should also describe the measures that will be taken to mitigate further adverse effects.

In addition to the obligation to notify the Dutch DPA, companies may also have to inform the affected individuals in the event of a data breach. This will be the case if it is likely that the data breach will have adverse effects on the data subject's privacy. An exemption from this obligation exists if the personal data have been encrypted or otherwise made unintelligible. The individuals must be informed where further information regarding the data breach may be obtained and also what measures will be taken to prevent additional negative consequences.

Companies must maintain a central register of all data breaches they experience. Failure to comply with this obligation will be subject to the same sanctions as the failure to make a timely report on a data breach to the Dutch DPA.

Violation of privacy regulations by major health insurance companies

The DPA has issued a warning to major health insurance companies for violation of privacy regulations. The insurance companies collected diagnosis data relating to clients through obtaining referral letters from doctors although the clients had issued specific privacy declarations purporting these data to be deleted from their invoices in order to avoid that the data would become available for the insurance companies.

PwC Netherlands annual Privacy Governance Survey

Over the past two years more than 150 organisations have participated in the Privacy Governance Survey. The Survey provides insight into how Dutch organisations deal with privacy, the importance they place on it and how they deal with current and upcoming data privacy regulations. It enables organisations to compare their privacy maturity and how they deal with the protection of personal data. It also provides insight into the organisations' readiness for the GDPR.

The Privacy Governance Survey has been proven to add value to Dutch organisations by contributing to a better understanding of the nature and impact of new privacy legislation, assessment of privacy risks, and an increased awareness of privacy governance and resilience within Dutch companies.

The Survey found that only 16% of the organisations condisderd themselves to be well or very well prepared for the new data breach notification requirement and more than 50% indicated that their investments in privacy compliance have increased over the past year.

Yvette van Gemerden
+31(0)88 792 54 42
yvette.van.gemerden@nl.pwc.com

Folkert Hendrikse
+31 (0)88 792 49 72
folkert.hendrikse@nl.pwc.com

Poland

In 2015, the Polish personal data protection authority (the General Inspector of Personal Data Protection, GIODO) received almost 1300 complaints from data subjects about how their personal data was being processed. Surprisingly, this figure is a significant decrease compared to previous years (nearly 2500 complaints in 2014, 1900 complaints in 2013 and 1600 complaints in 2012).

Another interesting point is that in 2015, the GIODO registered less than 9000 data filing systems, compared to nearly 16900 registered data filing systems in 2014. We believe that this decrease may relate to the fact that at the beginning of 2015, the Polish law on personal data protection changed. The new law expanded a list of exceptions from the obligation to register data filing systems.

Banks

Although the amount of decisions issued by the GIODO in 2015 has dropped we have noticed that the GIODO took a particular interest in the activity of the banking sector.

Under Polish law, banks are entitled to report their client's personal data to the bureau of credit information (in Polish: Biuro Informacji Kredytowej, BIK), where these clients have outstanding debts and on the condition that the banks have duly informed the clients about such reporting. The data may be kept in the bureau of credit information for 5 years following payment of the debt in full and are available to other banks during this period. Banks use this information to access the client's financial rating. As a result of a complaint filed by some of these clients, the GIODO looked into whether such reporting was compliant with Polish data protection law.

As was discovered, in some cases banks had not retained proof of informing clients about the reporting, with clients claiming that such information had not been provided at all, leaving the banks with no legal ground for processing clients' data for the period of 5 years after paying off the debt. The GIODO decided that although the banks are not obliged to keep the proof of complying with their information obligations, in the absence of such proof, banks are not able to successfully claim that the information obligation has been complied with. In addition, since the banks can not prove that they informed the clients, they also do not hold a valid ground for processing information about clients' debts for 5 years after settling the debt, and in consequence they are not entitled to report this information to the bureau of credit information. As a result, banks were obliged to delete this information from the database kept by the bureau of credit information (e.g. decision DOLiS/DEC-87/15/9908, 9910, 9920 and DOLiS/DEC-176/15).

A further case relating to the banking sector concerned the processing of a client's personal data for marketing purposes. It was held that the consent relied upon for such processing was forced, as when contacting the bank through its website, the client was requested to give this consent. It was not possible to contact the bank without giving this consent to process personal data for marketing purposes. The GIODO signaled that such consent may not be an effective ground for processing personal data as it was forced (DOLiS-035-304/15).

Publishing personal data relating to debts

This case related to the online publishing of personal data concerning the debt of an individual who conducted a business activity. The published personal data included: the name of the business activity (which included the first name and surname of this individual), zip code, the city, the street name and NIP number (tax identification number).

The company which published this information acquired the debt from the original creditor and was offering the debt for further sale.

As the Polish law applies to all personal information pertaining to an individual (also in case where such an individual conducts a business activity), the details published on the website were considered personal data.

The GIODO decided that, in order to successfully sell a debt, a data controller is entitled to publish information about this debt to an extent that allows for identification of the debtor. In relation to the legal ground for processing, the GIODO noted the "legally justified interest pursued by a data controller" and in particular "vindication of claims resulting from economic activity" (decision DOLiS/DEC-48/15/6615, 6623, 6627). Therefore, in the considered case the personal data were published on the website in compliance with Polish data protection law.

Other decisions

Other decisions of the GIODO related to data controllers not fulfilling information obligations towards data subjects; data controllers processing personal data in a manner not adequate for the purpose of processing; the proper defining of a data controller and a data processor (a company which offered sporting activities for employees of its clients claimed to be a data processor while GIODO decided that it was a data controller).

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

Russia

In 2015, personal data protection was a prominent topic for the Russian authorities. Enforcement agencies, such as Roskomnadzor (the authority in charge of control in the sphere of communications, information technologies and mass media) and Mincomsvyaz (the authority in charge of developing regulations on personal data processing), have taken an essential role in interpreting the requirements by communicating with business representatives and issuing clarifications.

Below is a high-level overview of some of the most important trends and activities in the sphere of personal data protection in Russia.

Localization requirement

A new law came into effect on 1 September 2015, which required personal data of Russian citizens to be collected, recorded, systematized, accumulated, stored, specified and extracted using informational databases located in Russia. Additionally, operators of personal data (i.e. individuals and entities that organize or effect processing of personal data and determine the purposes for which personal data are to be processed) must inform Roskomnadzor of the exact location of the above databases.

Roskomnadzor is empowered to include violators of the localization requirement in a state register of violators, as well as restrict access to the personal data that is processed in violation of the requirement by blocking a domain name of the relevant website, its network address and indexes of pages.

Mincomsvyaz has clarified that the localization requirement is applicable not only to a Russian legal entity, but also to any foreign legal entity that has a presence in Russia, or which carries out its activities in Russia. The latter includes, inter alia, having website information in Russian language and/or a Russian domain zone, addressing (advertising) such information to Russian customers, fulfilling a contract in the territory of Russia or having Internet platforms enabling payment of goods or services to take place in the Russian currency.

Officials of Roskomnadzor have declared that they are switching to the model of selective inspections of personal data operators, which shall be made based on measures of systematic monitoring, contrary to the previously established enforcement practice of massive inspections. Predominantly personal data operators that will be subject to monitoring and inspections are those which transfer personal data outside of Russia, process a significant amount of personal data (e.g. social networks, companies offering services to be rendered outside of Russia) or those who have been subject to complaints.

By the end of 2015, Roskomnadzor exposed three violations of the localization requirement. These violations are currently under the examination process.

The right to be forgotten

A new law, effective 1 January 2016, introduced the "right to be forgotten" concept to Russia. Under the law, an individual has the right to request illegally distributed, incorrect or outdated information related to the individual to be deleted from the Internet search engine's results. The law provides for a few exceptions from this rule, such as information about an event carrying indications of a criminal offense, limitations on convictions which have not expired, and the information about an individual committing a crime for which conviction is still outstanding.

The failure of an Internet search engine operator to comply with a writ of execution requesting them to remove the inclusion of such information from search results is subject to an administrative fine up to 1,000,000 Russian rubles (approximately 10 000 GBP).

Due to the importance of the issue, we expect that implementation of this right will intensify in 2016.

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

Spain

Safe Harbor

Following the ruling of the Court of Justice of the European Union (CJEU) of 6 October 2015 in the Maximilian Schrems v Data Protection Commissioner case (C-362/14), the Spanish Data Protection Agency (AEPD) called data controllers which had declared an international transfer of data to the USA before the 29th January 2016, to inform them about the continuity of such international transfers, and where relevant, about the adequacy of them. The AEPD warned that failure to provide a justification or to dully notify them of international transfers before the deadline may entail the temporary suspension of the international data transfers.

The Spanish Data Protection Agency issues the Strategy Plan 2015-2019

After receiving more than 400 responses from citizens during the public consultation, the AEPD has issued its Strategy Plan 2015-2019.

According to the legal forecasts, the Plan, which aims to develop or update more than twenty guides, includes the following overall objectives developed through concrete measures:

- Prevention activities, especially in areas with a major impact such as education and child protection, the treatment of data in the health sector or irregular recruitment.
- Initiatives that contribute to a climate of trust in the field of digital economy, promoting competitiveness and innovation.
- Proactive tasks to detect the potential impact of new technological developments on privacy.
- Projects which envision boosting communication with citizens.
- Improvement of the quality of services of the Agency.
- Response to international challenges within the framework of the European Data Protection Regulation.

2014 AEPD Annual Memory

In June 2015, the AEPD reported on its activities during 2014. The report showed an overall increase in the number of claims and complaints by over 15%. Video surveillance, fraudulent agreements, inclusion on financial solvency and creditworthiness files and debt collection related issues represented the most significant share of the claims.

Some of the key points of the Memory were:

- The AEPD replied to over 200,000 queries submitted by citizens;
- The telecommunication sector was the economic sector with a higher volume of sanctions, followed by financial institutions and companies supplying and marketing water and energy;
- Within the "right to be forgotten" claims, the Spanish Central Court (Audiencia Nacional) confirmed the criteria set out by the AEPD in 93% of cases.

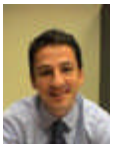
For the future, the AEPD points out the main "privacy challenges" as being Big Data and the Internet of Things, with a direct impact on the control of individuals over their information.

Financial penalties

Failure to comply with the Spanish data protection regulation results in an infringement of the regulation, irrespective of whether civil liability or criminal sanctions may result. Infringements, which are classified as minor, serious or very serious, are subject to a fine ranging from €900 to €600,000 respectively.

Although official figures and enforcement trends will not be released until midyear, we anticipate that the most significant financial penalties have been issued against companies belonging to energy and telecommunications sectors, such as:

- A multiple penalty against different telecommunication companies and a telemarketing provider as a consequence of the inaccurate processing of data and sending electronic communication without prior consent. The penalties ranged from €10,000 to a company that sent electronic communications without consent, to €50,000 to a telecommunication company which breached the security principle.
- A €100000 penalty against a telecommunication company which mistakenly provided a claimant's ID to a financial solvency and creditworthiness entity. Given that the company could not prove the origin of the data provided, the AEPD fined the company due to a serious breach of the data quality and information principles.



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

In Sweden the Data Inspection Board (DIB) has the responsibility to enforce the Personal Data Act, the Debt Recovery Act and the Credit Information Act. The DIB has been instructed to focus on sensitive areas, new trends and areas with big risks for privacy violations. They perform inspections in two ways; by visiting organisations in person, or by sending out a survey for the organisation to complete. As a part of the inspection, the DIB will often provide guidance on how an organization can improve its privacy policies and/or procedures.

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 act on 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 competence requirements. It is voluntary for an organisation to appoint a PDR, and if they do, they do not need to notify the Data Inspection Board that they process personal data. The PDR is expected to ensure that the organisation complies with the Personal Data Act by providing it with appropriate advice.

Enforcement actions

Below is a high level overview of the actions of the DIB in 2015:

- Camera surveillance: 19 (mostly retailers)
- Credit information: 3 (credit information companies)
- Debt Recovery: 17 (debt recovery companies and one electric power supplier)
- Personal Data: 64 (health care, research, the police, financial services, telecom and internet providers, public authorities, transportation companies, banks, schools, research organisations).

The most significant media story in 2015 was the EU Court of Justice Safe Harbour judgment, followed by the tripartite agreement on the final draft of the General Data Protection Regulation.

Prosecutions and appeals (2015 examples)

Background checks (January): Two companies performing screening and background checks appealed against a decision made by the DIB which found that their processing of personal data was covered by the Personal Data Act. The Supreme Administrative Court upheld the appeal on the basis of an exemption for 'unstructured' data, finding that the personal data shall not be deemed to have been structured to substantially facilitate the search or collection of data.

Court diary entries (July): The Supreme Court rejected an individual's request to electronically get as many Court of Appeal diary entries as possible from a particular year. The individual sought to apply the so-called individual exemption in the Personal Data Act (PDA), under which the PDA does not take account of a private person who processes personal data on his/her computer. The Court held that the exemption did not extend apply to this type of processing and no diary entries could be disclosed in electronic form.

Camera surveillance (August): The County Administration Board in Stockholm granted permission for camera surveillance by the police at several train stations in Stockholm, which was appealed by the DIB. The Administrative Court in Stockholm upheld the appeals on the basis that the interests of surveillance should be balanced with protecting integrity and, according to established practice, permissions should be granted restrictively. The Court found that, on balance and when taking into account that the monitoring was to take place around the clock and cover a large area, the privacy interests were more significant.

Log in details (September): The Administrati

t the Act does apply to such drones and therefore a permit is required when using a drone to video record in areas where the public has access.

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. Generally speaking, the number of data breaches reported to the PTS is very low.

In 2015, there has been continued upheaval over telecom operators' data retention requirements after the EU Directive on which the Swedish Electronic Communication Act is based was invalidated in 2014. In late 2014, the Administrative Court decided that the operators still had to provide traffic data to the PTS, which was a requirement under the invalidated EU Directive. Tele2, one of the impacted telecom operators, appealed the Administrative Court's decision.

The question now stands as to whether the Swedish rules on data retention are compatible with EU law and the Swedish Constitution, given that there is no longer an obligation to store traffic data. In May 2015, a request for a preliminary ruling was lodged with the EU Court of Justice.

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

Switzerland

Summary of the activities of the Federal Data Protection and Information Commissioner (FDPIC)

Transferring pseudonymised bank customer data outside Switzerland

In 2013, the Swiss Financial Market Supervisory Authority, FINMA, carried out a partial revision of its Circular – "Operational Risks – Banks". During the past year, FINMA focused on the fact that there was a discrepancy between the practical implementation of the 2008/7 Circular "Outsourcing Banks" and the position of the FDPIC. Most of the regulated financial institutions in Switzerland believe that they do not have a duty to specifically inform their clients about the outsourcing of their personal data after they have been pseudonymised. This is because the industry's position is that the data do not fall within the scope of the Swiss Data Protection Act (Swiss DPA).

This position is based on a diverging interpretation of the term pseudonymisation and "identifiability". According to the Swiss DPA, all data that are related to identified or identifiable persons qualify as personal data. The representatives of the financial industry came to the conclusion that pseudonymised data are not personal data within the meaning of the DPA because they cannot be correlated with identified or identifiable individuals. Any third party who has possession of the data will not have the necessary information to make re-identification possible.

The Federal Supreme Court decided (Logistep, BGE 136 II 508) that the Swiss DPA applies to bank customer data that are sent for processing outside Switzerland, which imposes a number of obligations on outsourcing banks. According to FINMA-RS 2008/7 "Outsourcing Banks", clients are to be informed in detail by a separate letter that their data are to be transferred abroad for processing purposes even if they are pseudonymised. In such circumstances, the customer must be also offered the opportunity to refuse the controversial clause (opt-out) or bring the contractual relationship to an end, without suffering any disadvantage as a result. In light of the risks involved, financial institutions have a responsibility to ensure that their clients are made aware of the kind of processing to which their data will be subject so that they may assert their self-determination rights.

Storing patients' records in the Cloud

Doctors are increasingly interested in storing patients' records in the Cloud. According to the Swiss DPA, the processing of personal data, and therefore the administration of patients' records, may be transferred to a third party. However, the data may only be processed in the way the data controller himself, i.e. the doctor, would be permitted to do. This applies even if there is no legal or contractual obligation to secrecy. As far as a patient's medical history or access to his medical record is concerned, doctors are bound by the legal obligation of professional secrecy. This obligation may not be transferred to third parties; but if such a transfer does take place, it must be covered by a contract. Consequently, the doctor remains entirely responsible for the processing of patient data.

The FDPIC is of the opinion that all doctors based in Switzerland who work with cloud-based service providers have only one choice: the cloud service providers and the cloud service have to be located in Switzerland, and they must be able to provide the doctor with a contractual guarantee that no patient records will be transferred outside the country. Consequently, a client-based encryption system must be used systematically for all patient data. In plain language, this means that the doctor, in his position as data controller, must be the only person to have the key to the data held in the cloud. The cloud service provider must not be able to obtain the key to unlock the data. The data controller/doctor may make the data available for statistical purposes, but only once he has made them totally anonymous.

Consultations in respect of the automatic exchange of tax information

After the adoption of the international OECD standard for automatic exchange of financial account information in tax matters, the FDPIC was asked to participate in the activities of the relevant working groups. The question of data protection is a key issue in this regard. One of the criticisms that has been levelled at the plan is the intention to use the Swiss social security number (AHV) as the tax identification number which would also be processed outside Switzerland. However, such use of the social security number would contravene the purpose limitation originally intended, and it significantly undermines privacy rights. The use of the AHV number for purposes outside the social security field would allow technical means to be used for unauthorised data linkage. In particular, it opens the door to personality profiling, identity theft, etc. As a reaction to the observations of the FDPIC, the plan to use the AHV number for the automatic exchange of tax information has now been abandoned. The FDPIC has been uncompromising in its demand that the automatic exchange of information must not undermine compliance with the principles of transparency and good faith. The Commissioner also insisted on the need to respect fundamental data protection values.

Copyright protection in cyberspace

Changes to Swiss copyright legislation will be examined and implemented. The FDPIC welcomes the fact that the current legal uncertainty regarding the procurement and processing of personal data in conjunction with cases of copyright infringement in cyberspace will thus be eliminated. However, the concern is to ensure that the measures that will be introduced take account of the need to protect individual privacy. The further legislative process will monitor it as it moves forward.

Susanne Hofmann
+41 58 792 1712
susanne.hofmann@ch.pwc.com

USA

2015 Privacy Enforcement Actions in the U.S.

Federal Trade Commission (more than $164,100,000 in penalties)

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:

- Two app developers will pay a combined $360,000 in civil penalties as part of settlements with the FTC over charges they violated the Children's Online Privacy Protection Act (COPPA). The terms of the settlements with the two developers require the defendants to pay civil penalties and comply with the requirements of COPPA in the future.
- A mobile service provider will pay $2.95 million in civil penalties to settle FTC charges that the company failed to give proper notice to consumers who were placed in a program for customers with lower credit scores and charged an extra monthly fee.
- The loan-servicing arm of an auto dealer will pay $82,777 in civil penalties as part of a settlement to address FTC charges that it failed to have written policies and procedures regarding the accuracy of reported credit information, and failed to properly investigate disputed consumer credit information.
- A discount retailer has agreed to pay $39.4 million to resolve claims by banks and credit unions that said they lost money because of the retailer's late 2013 data breach. The preliminary settlement resolves class-action claims by lenders seeking to hold the retailer responsible for their costs to reimburse fraudulent charges and issue new credit and debit cards.
- An identity theft protection service agreed to pay $100 million to settle FTC contempt charges that it violated a 2010 settlement with the agency and 35 state attorneys general by continuing to make deceptive claims about its identity theft protection services, and by failing to take steps required to protect its users' data.
- A federal court imposed a $1.7 million judgment against three defendants who took part in a scheme that used calls to numbers on the Do Not Call Registry and illegal robocalls to pitch bogus credit card interest rate reduction services to consumers struggling with debt.
- A mobile service provider agreed to pay $2.95 million in civil penalties to settle allegations that the company failed to give proper notice to consumers who were placed in a program for customers with lower credit scores and charged an extra monthly fee.
- An app developer and its principals agreed to pay $300,000 in civil penalties to settle charges that they violated COPPA. The FTC alleged that the company created a number of apps targeted to children and allowed third-party advertisers to collect children's personal information in the form of persistent identifiers through the apps. One advertising network over the course of 2013 and 2014 specifically warned the defendants about the obligations of the revised COPPA Rule, and also told the defendants that certain of their apps appeared to be targeted to children under the age of 13.
- The FTC and 10 state attorneys general sued a cruise company and its lead generators for illegally sending billions of political survey robocalls to sell cruise vacations. The cruise company and the lead generators have agreed to consent judgments totaling more than $13 million. Those settlements are awaiting court approval.
- At the FTC's request, a federal court imposed a $3.4 million judgment against an individual, a repeat offender, and his company for engaging in a telemarketing scheme that used deception, threats, and intimidation to induce elderly consumers to pay for medical alert systems they neither ordered nor wanted. The FTC alleged that defendants illegally placed calls to numbers on the Do Not Call Registry to reach elderly consumers – many of whom are in poor health and rely on others for help with managing their finances – and pressure them into buying a medical alert service.

Federal Communications Commission (more than $25,000,000 in penalties)

- The FCC Enforcement Bureau entered into a $595,000 settlement with a cable operator to resolve an investigation into the company's loss of customer personal data. The settlement represents the FCC's first privacy and data security enforcement action against a cable operator.
- The FCC fined a telecommunications corporation $25 million for failing to protect the personal information, including Social Security numbers, of its customers.

U.S. Department of Health and Human Services (more than $5,000,000) 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 2015:

- HHS settled with a management corporation for $3.5M concerning violations of HIPAA stemming from an investigation following multiple breaches of unsecured PHI.
- Federal regulators have announced an $850,000 HIPAA settlement with a hospital stemming from an investigation into the theft of a laptop that was used to operate a medical device.
- A large radiation oncology practice in Indianapolis, is reevaluating its privacy and security practices after it was slapped with a $750,000 HIPAA settlement from the Department of Health and Human Services. It agreed to pay the sum to settle alleged HIPAA violations involving a breach that occurred three years ago.

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

Team and contact information

UK Based Lawyers

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

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

Monica Sagado
Senior Manager
+44 (0)20 7212 4182
monica.salgado@pwclegal.co.uk

Polly Ralph
Senior Manager
+44 (0)20 7804 1611
polly.ralph@pwclegal.co.uk

David Cook
Manager
+44 (0)161 245 2485
d.cook@pwclegal.co.uk

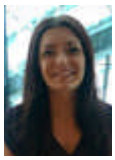
Jane Berry
Manager
+44 (0)20 7213 2450
jane.berry@pwclegal.co.uk

Joshua Fineman
Manager
+44 (0)20 7804 7792
joshua.fineman@pwclegal.co.uk

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

Emily Thompson
Senior Associate
+44 (0)7802 659 375
emily.thompson@pwclegal.co.uk

Teodora Pimpireva
Senior Associate
+44 (0) 20 7213 1430
teodora.pimpireva@pwclegal.co.uk



Lucy Tucker
Trainee Solicitor
+44 (0)20 7212 2299
lucy.c.tucker@pwclegal.co.uk

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

Tughan Thuraisingam
Trainee Solicitor
+44 (0) 207 804 3770
tughan.thuraisingam@pwclegal.co.uk

Oliver Pike
Trainee Solicitor
+44 (0) 207 804 2637
oliver.t.pike@pwclegal.co.uk

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

UK Risk Assurance, Consulting and Forensics

Jane Wainwright
+44 (0) 7715 034 015
jane.a.wainwright@uk.pwc.com

Mark Hendry
+44 (0) 7715 487 457
mark.hendry@uk.pwc.com

Jessica Tay
+44 (0) 7711 562 552
jessica.tay@uk.pwc.com

Craig Skinner
Craig.skinner@uk.pwc.com
+44 (0) 207 213 4588

Luther Teng
Luther.teng@uk.pwc.com
+44 (0) 207 213 3328

Radhika Bogahapitiya
+44 (0) 7454 638 153
radhika.p.bogahapitiya@uk.pwc.com

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

Angelica Pena
+44 (0) 7736 946 619
Angelica.pena@uk.pwc.com

Craig Fyfer
+44 (0) 7701 297 345
Craig.m.fyfer@uk.pwc.com

Phil Mennie
+44 7808 105525
philip.s.mennie@uk.pwc.com

Ula Krokay
+44 (0) 207 804 5043
ula.krokay@uk.pwc.com

Erin Anzelmo
+44 (0) 7702 698 859
erin.l.anzelmo@uk.pwc.com

Cal McGuire
+44 (0) 20 7804 3857
cal.mcguire@uk.pwc.com

Ian Todd
+44 (0) 207 8043 857
Ian.todd@uk.pwc.com

Angeliki Triantou
+44 (0) 207 213 3531
angeliki.triantou@uk.pwc.com

International Lawyers

Tony O'Malle
lia
+61 (2) 8266 3015
Tony.omalley@au.pwc.com

Benn Wogan
Australia
+61 (0) 7 3257 8124
benn.wogan@au.pwc.com

Yolanda Chorazyczewski
Australia
+61 (2) 8266 2471
yolanda.chora@au.pwc.com

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

Leen Van Goethem
Belgium
+32 2 710 78 76
leen.van.goethem@lawsquare.be

Ilya Komarevski
Bulgaria
+359 2 93 55 100
ilya.komarevski@tbk.bg

Jenny Zhong
China
+86 10 6533 2908
Jenny.j.zhong@cn.pwclegal.com

Raojuan Li
China
+86 (10) 6533 3073
raojuan.li@cn.pwclegal.com

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

Michael Chan
France
+33 (0)3 90 40 26 13
michael.chan@pwcavocats.com

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

Johannes Droste
Germany
+49 (0) 211 981 4805
johannes.droste@de.pwc.com

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

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

Filippo Zucchinelli
Italy
+39 051 6167736
filippo.zucchinelli@it.pwc.com

Filippo Riva
Italy
+39 02 91605224
filippo.riva@it.pwc.com

Yerkebulan Rakhmenov
Kazakhstan
+7 (727) 330 3200
Yerkebulan.rakhmenov@kz.pwc.com

Aija Panke
Latvia
+371 97094400
aija.panke@lv.pwclegal.com

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

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

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

Yvette van Gemerden
Netherlands
+31 (0)88 792 5442
yvette.van.gemerden@nl.pwc.com

Folkert Hendrikse
Netherlands
+31 (0)88 792 4972
folkert.hendrikse@nl.pwc.com

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

Slawomir Kowalski
Poland
+48 519 50 7837
Slawomir.kowalski@pl.pwc.com

Guillermo Zapata
Peru
+ (511) 211 6500
guillermo.zapata@pe.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

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

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

Assumpta Zorraquino Rico
Spain
+ 34 93 253 25 07
assumpta.zorraquino@es.pwc.com

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

Michael Meyer
Switzerland
+41 58 792 51 31
michael.adrian.meyer@ch.pwc.com

International Risk Assurance, Consulting and Forensics

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

Armando Colbourne
Australia
+61 (4) 1730 1672
Armando.a.colbourne@au.pwc.com

Leda Bargiotti
Belgium
+32 2 7104791
Leda.bargiotti@be.pwc.com

Tomas Clemente Sanchez
Belgium
+32 (0) 2 710 41 60
tomas.clemente.Sanchez@be.pwc.com

Nicolas Noël
Belgium
+32 491 86 40 83
nicolas.noel@be.pwc.com

Gaël Hachez
Belgium
+32 2 710 9617
Gael.hachez@be.pwc.com

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

David Craig
Canada
+1 416-814-5812
david.craig@ca.pwc.com

Carinna Lin
Canada
+1 416-869-2368
carinna.lin@ca.pwc.com

Adriana Gliga-Belavic
Canada
+1 416-815-5148
adriana.gliga@ca.pwc.com

Jordan Prokopy
Canada
+ 1 416 869 2384
Jordan.prokopy@ca.pwc.com

Jørgen Sørensen
Denmark
+45 3945 3554
jgs@pwc.dk

Patrick Qvick
Finland
+358 (0) 45 677 228
patrick.qvick@fi.pwc.com

Rajinder Singh
India
+91 9873264886
Rajinder.singh@in.pwc.com

Paul Graham
Japan
+81 (0) 80 4937 6267
Paul.p.graham@jp.pwc.com

Kenichi Kotaki
Japan
+81 (0) 80 3445 2028
kenichi.kotaki@jp.pwc.com

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

Maurice Steffin
Netherlands
+31 6 57 99 76 74
maurice.steffin@nl.pwc.com

Sandra Mochèl
Netherlands
+31 887923092
Sandra.Mochel@nl.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

Line Engebretsen
Norway
+47 982 14 600
Line.engebretsen@no.pwc.com

Tan Shong Ye
Singapore
+65 (0) 6236 3262
Shong.ye.tan@pwc.sg.com

Yap Yee Chin
Singapore
+65 (0) 6236 3351
yee.chin.yap@pwc.sg.com

Michelle Xie
Singapore
+65 (0) 6236 3351
michelle.qy.xie@sg.pwc.com

Pavol Adamec
Slovakia
+421 904 702339
Pavol.adamec@sk.pwc.com

Jordi Juan Guillem
Spain
+34 915 684 086
jordi.juan.guillem@es.pwc.com

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

Cecilia Cederberg
Sweden
+46 (0) 709 29 33 20
cecilia.cederberg@se.pwc.com

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

Björn Sieger
Switzerland
+41 (0) 794403524
bjoern.sieger@ch.pwc.com

Oktay Aktolun
Turkey
+90 212 326 60 73
oktay.aktolun@tr.pwc.com

Angela Saverice-Rohan
USA
+1 (213) 270 8913
angela.m.saverice-rohan@pwc.com

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

Privacy Shield

Helping you to build your Privacy Shield:

- Support with certifications
- Understanding the risks
- Solutions for cross-border transfers of personal data
- Responding to complaints
- Handling regulator scrutiny

Attend our GDPR Bootcamps

Join our GDPR Bootcamps every month by WebEx or in person.

We provide:

- Accessible insights into the requirements of the GDPR
- Pragmatic recommendations on how to operationalise the GDPR and reduce operational, legal and commercial risk
- Learning and networking opportunities with peers in your industry

We also offer tailored in-house GDPR training and awareness sessions