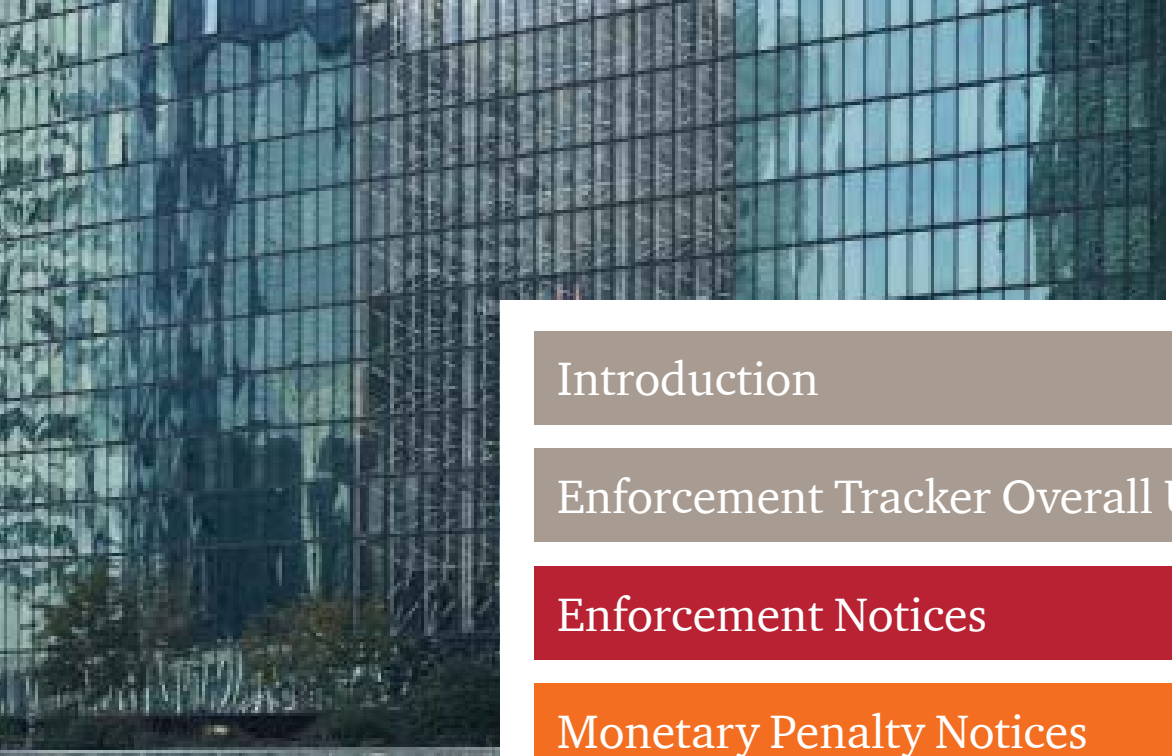
www.pwc.co.uk

Privacy and Security Enforcement Tracker 2016

May 2017

pwc



Introduction 04

Enforcement Tracker Overall UK Statistics 06

Enforcement Notices 07

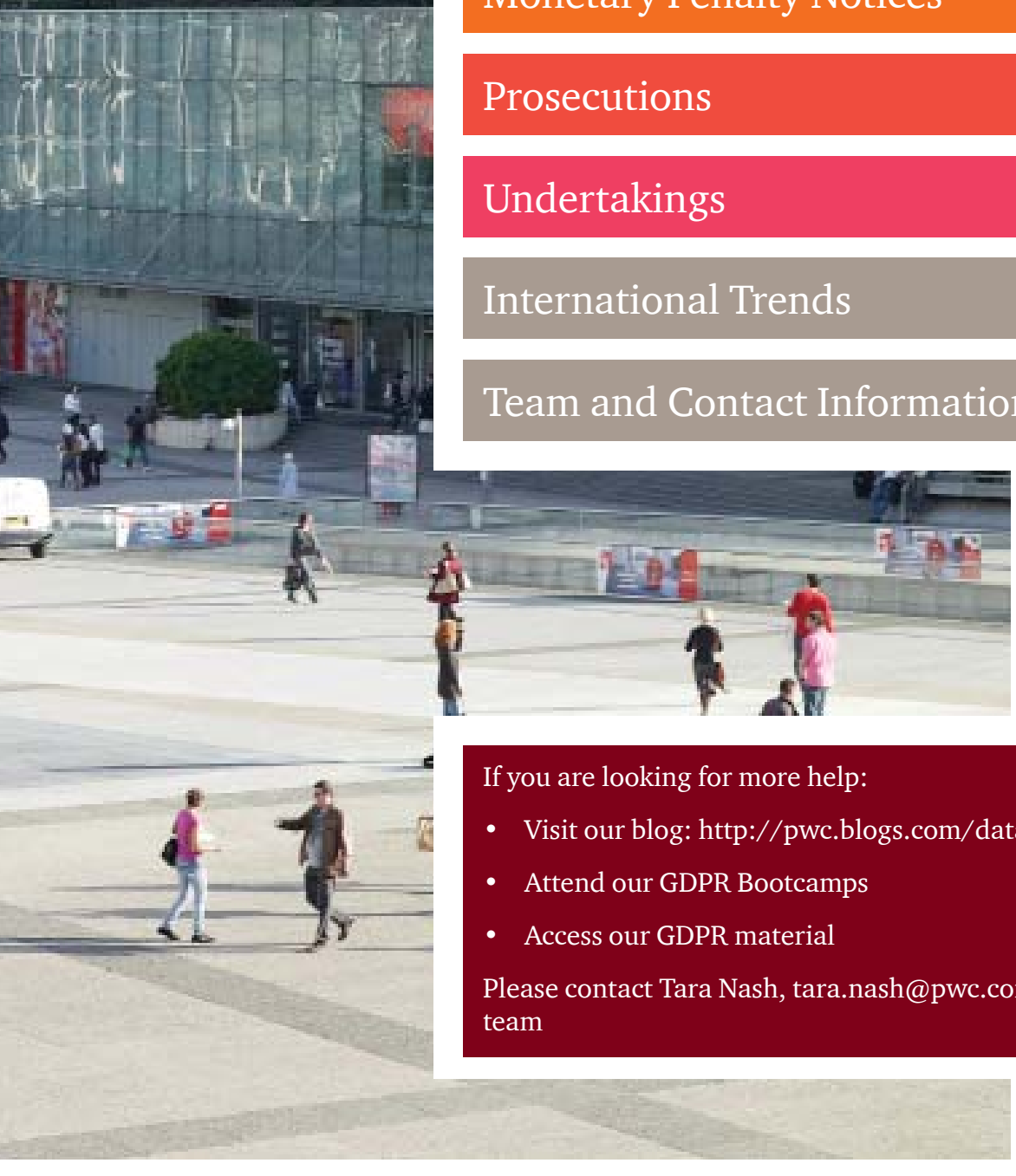
Monetary Penalty Notices 15

Prosecutions 36

Undertakings 40

International Trends 68

Team and Contact Information 99



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@pwc.com or any member of the team

2016: The year we tried to get ready for the new world of data protection

Welcome to the third annual PwC Privacy and Security Enforcement Tracker, where we review the key regulatory enforcement cases in the UK and in twenty other countries in 2016.

In all places where PwC's global data privacy team operates around the world, the big story of 2016 was the GDPR and the efforts being made by our clients to get ready. We performed countless maturity assessments using our GDPR Readiness Assessment Tool (The R.A.T.), we traced endless information lifecycles using our "data mapping" tools and we engaged with many hundreds of client stakeholders in "Vision-setting" workshops. During all this work one of the dominant themes in our client discussions was the likelihood of the GDPR triggering a regulatory enforcement and litigation storm: understandably, people are worried about the risk of mega fines and "class actions" - and of course, we recognise that many people may be seen to have vested interests in maintaining the impression that the GDPR is something to be very afraid of.

What will happen when the GDPR comes into force?

While we cannot pretend to have unique powers of foresight, we very much doubt that the GDPR will deliver immediate, extreme regulatory outcomes of the kind that some people are predicting, namely an explosion of fines at 4% of annual worldwide turnover soon after May 2018. Nor do we believe that the GDPR will be "another Y2K moment", whereby nothing actually happens. Instead, we anticipate a gradual build-up of challenges in the economy, due to: EU regulators undertaking "high profile" enforcement investigations into areas of most acute concern to them, such as online data processing; a growing number of "class actions", compensation claims and litigation pursued by individuals, workers representatives and privacy advocates; and companies enforcing the GDPR through their supply chains.

As far as regulatory enforcement action is concerned, a large part of our reasoning is based on the evidence that we have gathered over the years on privacy and security regulatory enforcement trends in Europe. The European pattern over the long term has been low volumes of regulatory enforcement actions, with low level financial penalties. In contrast, the United States, has for a number of years imposed financial penalties far in excess of anything in Europe. In this year's Enforcement Tracker the United Kingdom, Italy and Spain stand out as the most active regions for regulatory enforcement action in Europe. The UK imposed fines totalling just short of £3.25 million, while Italy imposed a total of EUR 3.3 million. In contrast, the total amount of fines imposed in the US was approximately $250 million. The European regulators have more in their regulatory toolkit than just headline grabbing enforcement powers, however.

Of course, we recognise that in an environment where fines are capped at a relatively low level (for example, the cap in the UK is currently £500,000), it will take a large effort to reach the fining levels experienced in the US, so perhaps it is unfair to judge a territory's "toughest" by financial metrics alone. A better indicator might be the total output of enforcement work. At first blush, this metric might suggest that the European data protection regulatory enforcement regime presents little to fear for most entities. We dispute this and we do not want to suggest that the regulators are not doing a good job, or that they do not have an appetite for difficult cases. Low levels of regulatory output might simply be the result of limited resources and weak powers. Of course, the GDPR will solve the power problem and if

the regulators are equipped with sufficient resources to do their jobs, their new powers will present a serious risk to organisations that fail to take GDPR seriously. We will be watching this space very closely.

We also argue that the GDPR has already made a real and lasting difference. It has brought data protection to much wider attention and it has certainly engaged the minds of our clients, who are making good efforts to meet the new requirements. In this sense, the GDPR should be seen as a force for good. After all, who can argue against a renewed approach to data protection and operational adequacy, where risk assessments, data assets registers, privacy by design philosophies and the like are part of business-as-usual activities? In our view, the GDPR provides a code for good business, which is why it is being embraced by our clients.

Of course, we should not forget that the GDPR is law. Law needs to be complied with. It is not an elective issue. For this reason alone, GDPR needs to be embraced.

Finally, we should not forget the E-Privacy Directive. 2016 saw the commencement of the law reform process to bring this regime into conformity with the GDPR. Europe is aiming to complete this reform before May 2018, so that both regimes come into effect at the same time.

The wider world – it's not just the EU that is legislating

Our multi-disciplinary data privacy practice operates all over the world, which gives us insights into how the laws are developing elsewhere. GDPR was not the only story of 2016: as you'll see from our digest, there were new developments in many countries, such as Australia, Canada, China, Japan and Mexico. In the US, President Trump's election hinted at a new approach to the privacy rights of non-US citizens, which we will be monitoring closely.

Privacy Shield – more legal challenges to international transfers

Continuing with the US and EU relationship, 2016 saw the European Commission adopt the Privacy Shield Decision, the successor to Safe Harbour. It had a controversial start to its life, with hesitation at the Article 29 Working Party's side. It is now being challenged before the European Court of Justice, just like the Model Clauses. Our multinational clients are hoping for legal certainty, one way or the other. We await the outcome with baited breath.

Brexit

Of course, we cannot ignore Brexit, which will take the UK outside the EU, making the UK a "third country" as far as the EU is concerned. We were honoured to have been involved in the UK Parliamentary inquiries into the impact of Brexit in the context of the GDPR and we look forward to sharing more insights with you, once the Parliamentary report is published. Based on the publicly available information, GDPR will be part of UK law, come what may.

Conclusions

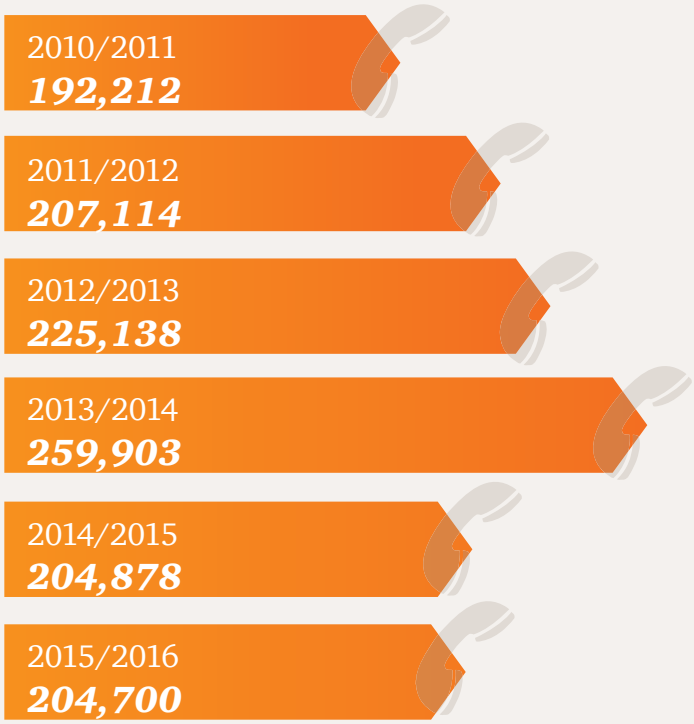
However we look at it and whatever our personal and business perspectives, none of us can ignore the impact of legal and regulatory change in this area. The past five years have changed the landscape beyond all recognition. It's obvious that data protection's time has arrived.

If you want to keep updated on developments, please contact any of our global leaders. We hold regular client seminars, workshops and conferences and have an abundance of learning literature that we will be happy to share with you. If you need any support addressing your data protection challenges, our global, multi-disciplinary team can help you on any matter, wherever you are.

Stewart Room
Partner
Co-Global Leader, PwC Data Protection Practice; Global Cyber Security And Data Protection Legal Services Leader; UK Data Protection Leader
+44 (0) 20 7213 4306
stewart.room@pwc.com
@StewartRoom

Jay Cline
Co-Global Leader, PwC Data Protection Practice; USA Data Protection Leader
+1 (612) 596 6403
jay.cline@pwc.com

Helpline calls received by ICO:



(Source:
Information Commissioner's Office ("ICO") Annual Operational Reports 2016/7
ICO Annual Report and Financial Statements 2015/16 printed on 28 June 2016
ICO Annual Report and Financial Statements 2014/15 printed on 30 June 2015
ICO Annual Report and Financial Statements 20 13/14 printed on 14 July 2014
ICO Annual Report and Financial Statements 2012/13 printed on 19 June 2013
ICO Annual Report and Financial Statements 2011/12 printed on 4 July 2012)

Enforcement activities in 2016 by sector

Prosecutions are excluded

Enforcement in the UK: analysis of statistics 2012-2016

	Monetary Penalty Notices	Prosecutions	Enforcement 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
2016	35	16	23	30	104

The importance of data privacy to consumer trust

90% of CEOs consider that breaches of data privacy and ethics will impact negatively on stakeholder trust levels in their industry to some extent or to a large extent

65% 64% of CEOs consider that how they manage people's data will differentiate them from the competition

(Source: PwC 20th CEO Survey 2017)

The emphasis on risk detection

of respondents say they actively monitor and analyse threat intelligence to help detect risks and incidents

(Source: PwC's The Global State of Information Security© Survey 2017)

Enforcement Notices

Total	***23***
Public Sector	***2***
Private Sector	***21***

The Alzheimer's Society

5 January 2016

No Monetary Penalty

DPA – 5th & 7th Principles

The ICO found serious failings in the way volunteers at a national dementia support charity handled sensitive personal data.

It ordered The Alzheimer's Society to take action after discovering that volunteers were using personal email addresses to receive and share information about people who use the charity, storing unencrypted data on their home computers and failing to keep paper records locked away.

Furthermore, volunteers were not trained in data protection, the charity's policies and procedures were not explained to staff and the volunteers had minimum supervision from charity staff.

Enforced remedial action required within 6 months:

1. Personal data is not to be kept for longer than is necessary;
2. Implement a mandatory data protection training programme for all staff (including volunteers who have access to personal data) and conduct refresher training at least every two years. Delivery of the training should be tailored to reflect the needs of both staff and volunteers;
3. Completion of any such training is monitored and properly documented;
4. Policies and procedures relating to data protection and information governance are brought to the attention of all staff (including volunteers who have access to personal data);
5. Portable and mobile devices including laptops and other portable media used to store and transmit personal data, the loss of which could cause damage or distress to individuals, are all encrypted using encryption software which meets the current standard or equivalent;
6. Secure email accounts are provided to all staff (including volunteers who process personal data by email in connection with their work for the data controller);
7. Secure storage is provided for all staff (including volunteers who hold hard copy records containing personal data in connection with their work for the data controller);
8. Manual (as well as automated) checks are conducted to identify vulnerabilities on the data controller's website e.g. penetration testing;
9. Appropriate organisational and technical measures are taken against the unauthorised access by staff (including volunteers) to personal data; and
10. Paragraphs 11 and 12 of Part II of Schedule 1 to the Data Protection Act ("DPA") are complied with where processing of personal data is carried out by a data processor on behalf of the data controller.

The Mint Condition Media Ltd trading as Hot Leads Factory

19 January 2016

No Monetary Penalty

DPA – 6th Principle

The Mint Condition Media Ltd trading as Hot Leads Factory was ordered to respond to a subject access request after the ICO ruled that it had failed to comply with the requirements of section 7 of the Data Protection Act.

Enforced remedial action required within 30 days:

1. Inform the individual making the request whether Hot Leads Factory holds the information requested and provide a copy of such information.

Types of Breach per legislation

PECR breaches: ***12***

Data Protection Act (DPA) breaches: ***11***

Martyn F Arthur Forensic Accountant Ltd

19 January 2016

No Monetary Penalty

DPA – 6th Principle

Martyn F Arthur Forensic Accountant Ltd was ordered to respond to a subject access request after the ICO ruled that it had failed to comply with the requirements of section 7 of the Data Protection Act.

Enforced remedial action required within 30 days:

1. Inform the individual making the request whether Martyn F Arthur Forensic Accountant Ltd holds the information requested and provide a copy of such information.

Preferred Pension LLP

24 February 2016

No Monetary Penalty

PECR – Regulations 19 & 24

Preferred Pension LLP was handed a legal "stop" order by the ICO after it was found that they had sent or instigated the sending of millions of nuisance calls / communications for the purposes of direct marketing.

Enforced remedial action required within 35 days:

1. Neither transmit, nor instigate the transmission of, unsolicited communications for the purposes of direct marketing by means of an automated call unless the recipient of the automated call has previously notified Preferred Pension LLP that he/she consents for the time being to such communications being sent by, or at the instigation of Preferred Pension LLP.
2. Neither transmit, nor instigate the transmission of a communication for the purposes of direct marketing by means of an automated call unless the name of the sender and either the address or telephone number (on which they can be reached free of charge) are included in that communication.

Advanced VoIP Solutions Ltd

24 February 2016

No Monetary Penalty

PECR – Regulations 19 & 24

Advanced VoIP Solutions Ltd was handed a legal "stop" order by the ICO after it was found that they had sent or instigated the sending of millions of nuisance calls / communications for the purposes of direct marketing.

Enforced remedial action required within 35 days:

1. Neither transmit, nor instigate the transmission of, unsolicited communications for the purposes of direct marketing by means of an automated call unless the recipient of the automated call has previously notified Advanced VoIP Solutions Ltd that he/she consents for the time being to such communications being sent by, or at the instigation of Advanced VoIP Solutions Ltd.
2. Neither transmit, nor instigate the transmission of a communication for the purposes of direct marketing by means of an automated call unless the name of the sender and either the address or telephone number (on which they can be reached free of charge) are included in that communication.

Types of breach of DPA
(includes 2 actions where breach of more than 1 DPP):

PECR breaches: ***12***

Data Protection Act (DPA) breaches: ***11***

Money Help Marketing Ltd

24 February 2016

No Monetary Penalty

PECR – Regulations 19 & 24

Money Help Marketing Ltd was handed a legal "stop" order by the ICO after it was found that they had sent or instigated the sending of millions of nuisance calls / communications for the purposes of direct marketing.

Enforced remedial action required within 35 days:

1. Neither transmit, nor instigate the transmission of, unsolicited communications for the purposes of direct marketing by means of an automated call unless the recipient of the automated call has previously notified Money Help Marketing Ltd that he/she consents for the time being to such communications being sent by, or at the instigation of Money Help Marketing Ltd.
2. Neither transmit, nor instigate the transmission of a communication for the purposes of direct marketing by means of an automated call unless the name of the sender and either the address or telephone number (on which they can be reached free of charge) are included in that communication.

Wainwrights Estate Agents Limited

3 March 2016

No Monetary Penalty

DPA – 6th Principle

Wainwrights Estate Agents Limited was ordered to respond to a subject access request after the ICO ruled that it had failed to comply with the requirements of section 7 of the Data Protection Act.

Enforced remedial action required within 30 days:

1. Inform the individual making the request whether Wainwrights Estate Agents Limited holds the information requested and provide a copy of such information.

F.E.P. Heatcare Ltd

14 March 2016

MPN issued on 14 March 2016 for £180,000

PECR – Regulations 19 & 24

Boiler replacement company – F.E.P. Heatcare Ltd – was fined by the ICO after it made 2.6 million unwanted calls and became listed as one of Britain's most complained about nuisance callers. The calls sent by F.E.P. Heatcare played a recorded message promoting the company's products and services.

Enforced remedial action required within 35 days:

1. Neither transmit, nor instigate the transmission of, unsolicited communications for the purposes of direct marketing by means of an automated call unless the recipient of the automated call has previously notified FEP Heatcare Ltd that he/she consents for the time being to such communications being sent by, or at the instigation of FEP Heatcare Ltd.
2. Neither transmit, nor instigate the transmission of a communication for the purposes of direct marketing by means of an automated call unless the name of the sender and either the address or telephone number (on which they can be reached free of charge) are included in that communication.

Types of breach of PECR:

Breach of PECR Regulation 21: ***3***

Breach of PECR Regulation 22: ***3***

Breach of PECR Regulations 19 & 24: ***5***

Breach of PECR Regulations 22 & 23: ***1***

Direct Choice Home Improvements Limited

21 March 2016

MPN issued on 21 March 2016 for £50,000

PECR – Regulation 21

The ICO 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 Direct Choice Home Improvements Limited.

The ICO previously notified Direct Choice Home Improvements Limited that such calls should not be made on that line and/or they had to register their number with the TPS.

Direct Choice Home Improvements Limited said a third party was to blame; telling the ICO it had been assured its list of people to call was screened against the TPS register. However, the ICO found that Direct Choice Home Improvements Limited had breached Regulation 21 of PECR.

Enforced remedial action required within 35 days:

1. Neither use, nor instigate the use of, a public electronic communications service for the purposes of making unsolicited calls for direct marketing purposes where the line called is that of a subscriber who has:
   a. previously notified the Direct Choice Home Improvements Limited that such calls should not be made on that line; and/or
   b. registered their number with the TPS at least 28 days prior to such call and has not notified Direct Choice Home Improvements Limited that they do not object to such calls being made.

Falcon & Pointer Limited

21 March 2016

MPN issued on 21 March 2016 for £175,000

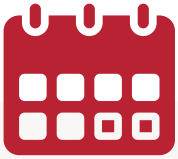
PECR – Regulations 19 & 24

Falcon & Pointer Limited, which had its license revoked by the Claims Management Regulator in January 2016, told the ICO it had stopped making calls in June 2015 but an investigation discovered it made a further two million automated calls in the following two months.

Falcon & Pointer Limited also did not identify itself as the organisation who was sending or instigating the automated marketing calls or provide an address or a telephone number on which it could be reached free of charge.

Enforced remedial action required within 35 days:

1. Neither transmit, nor instigate the transmission of, communications comprising recorded matter for direct marketing purposes by means of an automated calling system except:
   a. where the called line is that of a subscriber who has previously notified the Company that for the time being he consents to such communications being sent by, or at the instigation of, the Company; and
   b. where the communication includes the name of the Company and either the address of the Company or a telephone number on which the Company can be reached free of charge.



Number of Enforcement Notices issued per year that resulted in a MPN being issued:

2016: ***5***

2015: ***1***

M I Wealth Management Ltd

18 March 2016

No Monetary Penalty

DPA – 6th Principle

M I Wealth Management Ltd are a financial advisors and wealth management business. They failed to respond to a subject access request made by an individual on 17 September 2015 in compliance with the requirements of section 7 of the DPA.

Enforced remedial action required within 30 days:

1. Inform the individual making the request whether M I Wealth Management Ltd holds the information requested and provide a copy of such information.

West Dunbartonshire Council

26 April 2016

No Monetary Penalty

DPA – 7th Principle

Following a security breach that occurred on 21 July 2014 the ICO carried out an investigation into West Dunbartonshire Council's compliance with the provisions of the DPA. The ICO found that the Council had failed to take appropriate technical and organisational measures against the unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Enforced remedial action required within 6 months:

1. Implement a mandatory data protection training programme for all staff (including new starters) and conduct refresher training on an annual basis;
2. Completion of such training should be properly documented and monitored to ensure training is completed within an appropriate timeframe;
3. Implement a home working policy to provide sufficient guidance for staff working remotely. A risk assessment should also be incorporated in the home working procedure to cover security of equipment.

Debbie Urch t/a Kings Ransom

6 June 2016

No Monetary Penalty

DPA – 6th Principle

Kings Ransom are a debt recovery and debt collection business. They failed to respond to a subject access request made by an individual on 17 September 2015 in compliance with the requirements of section 7 of the DPA.

Enforced remedial action required within 30 days:

1. Inform the individual making the request whether Kings Ransom holds the information requested and provide a copy of such information.

Central Compensation Office Limited

6 June 2016

No Monetary Penalty

PECR – Regulation 21

The ICO received 167 complaints via the TPS, and 23 directly from individuals who were subscribers to specific telephone lines, in relation to unsolicited marketing calls from the Central Compensation Office Limited. The complaints were received despite the ICO previously notifying Central Compensation Office Limited that such calls should not be made on that line and/or that they had to register 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 purposes of making unsolicited calls for direct marketing purposes where the line called is that of a subscriber who has:
   a. previously notified the Central Compensation Office Limited that such calls should not be made on that line; and/or
   b. registered their number with the TPS at least 28 days prior to such call and has not notified Central Compensation Office Limited that they do not object to such calls being made.

Change and Save Ltd

6 July 2016

No Monetary Penalty

PECR – Regulation 21

Change and Save Ltd was handed a legal "stop" order by the ICO after the ICO received a number of complaints via the TPS and directly from individuals in relation to unsolicited marketing calls from Change and Save Ltd. The complaints were received despite the ICO previously notifying Change and Save Ltd that such calls should not be made on that line and/or they had to register 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 purposes of making unsolicited calls for direct marketing purposes where the called line is that of:
   a. a subscriber who has previously notified the Company that such calls should not be made on that line; and/or
   b. a subscriber who has registered their number with the TPS at least 28 days previously and who has not notified the Company that they do not object to such calls being made.

Consumer Finance Claims Ltd

7 July 2016

No Monetary Penalty

DPA – 6th Principle

Consumer Finance Claims Ltd is a claims management company specialising in PPI. They failed to respond to a subject access request made by an individual on 29 June 2015.

Enforced remedial action required within 30 days:

1. Inform the individual making the request whether Consumer Finance Claims Ltd holds the information requested and provide a copy of such information.

London Borough of Lewisham

26 July 2016

No Monetary Penalty

DPA – 6th Principle

The London Borough of Lewisham failed to respond to a subject access request made by an individual on 8 July 2015 in compliance with section 7 of the DPA.

Enforced remedial action required within 30 days:

1. Inform the individual making the request whether London Borough of Lewisham holds the information requested and provide a copy of such information.

Nottingham Forest Football Club Ltd

26 July 2016

No Monetary Penalty

DPA – 6th Principle

Nottingham Forest Football Club - a professional English football team - failed to respond to a subject access request made by an individual on 11 November 2015 in compliance with the requirements of section 7 of the DPA.

Enforced remedial action required within 30 days:

1. Inform the individual making the request whether Nottingham Forest Football Club Ltd holds the information requested and provide a copy of such information.

Poundstretcher Limited

5 September 2016

No Monetary Penalty

DPA – 6th Principle

Poundstretcher Limited failed to respond to subject access requests made by an individual on 3 and 10 March 2016 in compliance with the requirements of section 7 of the Data Protection Act.

Enforced remedial action required within 30 days:

1. Inform the individual making the request whether Poundstretcher Limited holds the information requested and provide a copy of such information.

Intelligent Lending Limited t/a Ocean Finance

27 September 2016

No Monetary Penalty

PECR – Regulation 22

The ICO issued Intelligent Lending Limited, trading as Ocean Finance, with an enforcement notice ordering it to stop sending spam texts. The credit card products broker used a public telecommunications service for the purpose of instigating 4,531,824 unsolicited direct marketing text messages.

Enforced remedial action required within 35 days:

1. Neither transmit, nor instigate the transmission of, unsolicited communications for the purposes of direct marketing by means of electronic mail unless the recipient of the electronic mail has previously notified Intelligent Lending Limited t/a Ocean Finance that he consents to such communications being sent by, or at the instigation of Intelligent Lending Limited t/a Ocean Finance.

Nouveau Finance Ltd

3 November 2016

MPN issued on 3 November 2016 for £70,000

PECR – Regulations 22 & 23

Nouveau Finance Ltd was handed a legal "stop" order by the ICO after it used a public telecommunications service for the purpose of instigating the transmission of 2.2 million unsolicited marketing text messages without the consent of subscribers. Nouveau Finance Ltd was subsequently fined £70,000 by the ICO.

Enforced remedial action required within 35 days:

1. Neither transmit, nor instigate the transmission of, unsolicited communications for the purposes of direct marketing by means of electronic mail unless the recipient of the electronic mail has previously notified Nouveau Finance Ltd that he consents to such communications being sent by, or at the instigation of the Nouveau Finance Ltd.
2. Neither transmit, nor instigate the transmission of, a communication for the purpose of direct marketing by electronic mail unless the name of the sender and either the address or telephone number (on which they can be reached free of charge) are included in that communication.

Key Insolvency Services Limited

23 November 2016

No Monetary Penalty

PECR – Regulation 22

Key Insolvency Services Limited was handed a legal "stop" order by the ICO after it instigated the transmission of 136 unsolicited communications by means of electronic mail to individual subscribers for the purposes of direct marketing. The text messages were sent by Key lead Solutions Ltd on behalf of Key Insolvency Services Limited and they did not have the consent of the 136 subscribers to whom it sent the unsolicited direct marketing text messages.

Enforced remedial action required within 35 days:

1. Neither transmit, nor instigate the transmission of, unsolicited communications for the purposes of direct marketing by means of electronic mail unless the recipient of the electronic mail has previously notified Key Insolvency Services Limited that he consents to such communications being sent by, or at the instigation of Key Insolvency Services Limited.

Silver City Tech Limited

29 November 2016

MPN issued on 25 November 2016 for £100,000

PECR – Regulation 22

Silver City Tech Limited was one of two companies responsible for sending millions of spam texts offering easy access to loans.

The ICO investigations found that Silver City Tech Limited did not have the consent of the people the text messages were sent to.

Enforced remedial action required within 35 days:

1. Neither transmit, nor instigate the transmission of, unsolicited communications for the purposes of direct marketing by means of electronic mail unless the recipient of the electronic mail has previously notified Silver City Tech Limited that he consents to such communications being sent by, or at the instigation of the Silver City Tech Limited.
2. Neither transmit, nor instigate the transmission of, a commission for the purposes pf direct marketing by electronic mail unless the name of the sender and either the address or telephone number (on which they can be reached free of charge) are included in that communication.

Monetary Penalty Notices (MPNs)

Total	***35***
Private Sector	***29***
Public Sector	***6***
Total Value	***£3,245,500***

MyIML Ltd

15 February 2016

MPN issued on 15 February 2016 of £80,000

PECR - Regulation 21

MyIML Ltd is a company whose business involves making unsolicited marketing calls to individual subscribers, in order to sell solar panels and other green energy saving equipment. Between 9 October 2013 and 17 July 2015, MyIML Ltd made 1048 unsolicited calls for direct marketing purposes to subscribers registered with the TPS opt out list. MyIML Ltd relied on personal data from third parties without undertaking due diligence. After a warning and a period of monitoring, complaints about MyIML Ltd continued.

The ICO found that it was inherently likely that a substantial amount of distress would arise from these calls, given the large number of affected individuals. As MyIML Ltd relied heavily on direct marketing for its business, and because the issue of unsolicited calls was widely publicised by the media, MyIML Ltd should have been aware of their responsibilities in this area.

Aggravating Factors:

1. MyIML Ltd may obtain a commercial advantage over its competitors by generating leads from unlawful marketing practices.
2. MyIML Ltd failed to suppress numbers when requested to do so.

Mitigating Factors:

1. There is a potential for damage to MyIML Ltd's reputation, which may affect future business.

Remedial Action:

No mention of remedial action.

Direct Security Marketing Ltd

15 February 2016

MPN issued on 17 February 2016 of £70,000

PECR – Regulation 19

Direct Security Marketing is a company that provides a range of marketing services to its clients. On 24 August 2015, Direct Security Marketing Ltd instigated 39,214 automated marketing calls regarding the purchase of security systems to subscribers of the TPS. 9775 of these calls were made between the hours of 01:00 and 06:00. The Commissioner's office received 49 complaints regarding these early morning calls via the online reporting tool.

The ICO contacted Direct Security Marketing Ltd to notify it of its obligations under the PECR and to provide it with an opportunity to give an explanation for the calls. Direct Security Marketing Ltd confirmed that it was the instigator of the calls, admitted that it did not have the prior consent of subscribers and stated that it was not aware that a different PECR regulation applied to automated marketing calls.

The ICO found that these early morning calls would be particularly disconcerting for subscribers. Also, given the detailed guidance issued by the ICO to companies carrying out marketing, Direct Security Marketing Ltd should have been aware of its responsibilities. Direct Security Marketing Ltd instigating automated marketing calls on a large scale to subscribers was deliberate.

Aggravating Factors:

1. The contravention was likely to cause substantial distress to the subscribers.
2. Direct Security Marketing Ltd may obtain a commercial advantage over its competitors by generating leads from unlawful marketing practices
3. The ICO noted that the person sending or instigating automated marketing calls was not identified, and an address or a number at which the person could be reached free of charge was not provided in breach of PECR Regulation 24.

Mitigating Factors:

1. Direct Security Marketing Ltd has fully co-operated with the ICO.
2. There is a potential for damage to the Company's reputation which may affect future business.

Remedial Action:

No mention of remedial action.

Types of Breach per legislation:

Breach of DPA 1st & 2nd principles: ***2***

Breach of DPA 7th principle: ***9***

Breach of PECR Regulation 19: ***9***

Breach of PECR Regulation 21: ***4***

Breach of PECR Regulation 22: ***8***

Breach of PECR Regulations 22 & 23: ***1***

Breach of PECR Regulation 5A: ***2***

Prodial Ltd

24 February 2016

£350,000

PECR – Regulation 19

Prodial Ltd is a company that generates leads in relation to individuals making a claim for a payment protection insurance refund. Prodial Ltd was responsible for over 46 million automated marketing calls. Between 30 January and 4 September 2015, the ICO office received 1,122 complaints via the online reporting tool. The calls did not identify the sender and an option of speaking to a person or suppressing the number was not always effective.

The ICO contacted Prodial Ltd to notify it of its obligations under the PECR and asked it to provide evidence of prior consent to receiving the automated marketing calls from the recipients. Prodial Ltd informed the ICO that it had purchased "opt-in" data from a reputable supplier, and that data had been screened against the TPS list. However, it could not produce evidence of prior consent.

Given the detailed guidance issued by the ICO to companies carrying out marketing, Prodial Ltd should have been aware of it responsibilities. The ICO held that Prodial Ltd had deliberately contravened PECR Regulation 19.

Aggravating Factors:

1. Prodial Ltd may obtain a commercial advantage over its competitors by generating leads from unlawful marketing practices.
2. The person sending or instigating automated marketing calls was not identified, and an address or a number at which the person could be reached free of charge was not provided.

Mitigating Factors:

There were no mitigating features.

Remedial Action:

No mention of remedial action.

David Lammy MP

10 March 2016

£5,000

PECR – Regulation 19

Mr David Lammy is an MP of the English House of Commons. He used an automated calling system for the purpose of making recorded direct marketing calls, to seek support for his bid to become the Labour Party's London Mayoral candidate. The ICO wrote to Mr Lammy, to give him an opportunity to provide an explanation for the automated calls and to warn him of potential civil monetary penalties. Mr Lammy confirmed that he had instigated a total of 35,629 automated calls to registered members of the Labour party.

The ICO found that the privacy policy Labour members agreed to did not contain information about automated direct marketing calls. No prior consent was given by Labour members to the phone calls instigated by Mr David Lammy.

The ICO found that it was reasonable that Mr Lammy should have been aware of his responsibilities in this area, because the ICO had published detailed guidance for those carrying out marketing. Also, the company he contracted made it clear to customers that prior consent was required for automated marketing calls. Mr Lammy did not take reasonable steps to prevent the contraventions.

Aggravating Factors:

No mention of aggravating features.

Mitigating Factors:

1. Mr Lammy fully co-operated with the ICO's investigation.
2. The calls were not made for commercial gain.
3. The contravention was a "one-off" and not part of a series of similar contraventions.
4. The ICO received only one complaint about the calls made.
5. The contravention was unlikely to cause distress to recipients of the automated calls, who were members of the Labour party.

Remedial Action:

No mention of remedial action.

Take our GDPR R.A.T

(Readiness Assessment Tool)

- ***70*** questions
- ***1*** maturity matrix
- ***2*** domains – architecture and principles
- ***2*** hours

Gives you full insight into your GDPR readiness

F.E.P. Heatcare Limited ("FEP")

14 March 2016

£180,000

PECR – Regulation 19

FEP is a Glasgow boiler company that sent unsolicited direct marketing calls regarding boiler replacements to TPS subscribers. The company instigated the sending of 2,692,217 automated marketing calls to subscribers on the TPS list. Between 18 June 2015 to 5 September 2015, the ICO received 94 complaints. The calls did not identify the sender or instigator of the call.

The ICO contacted FEP to notify it of its obligations under the PECR and warned it that the ICO could issue civil monetary penalties for non-compliance. FEP replied, stating that the automated calls were not made by FEP but by a separate company set up by a representative of FEP to deal with marketing activities. It confirmed that it had no evidence of prior consent from the recipients.

The ICO found that it was reasonable that FEP should have been aware of their responsibilities in this area, because the ICO had published detailed guidance for those carrying out marketing.

The ICO held that a monetary penalty in this case should act as a general encouragement towards compliance with the law, or at least as a deterrent against non-compliance, on the part of all persons running businesses currently engaging in these practices.

Aggravating Factors:

1. The ICO had previously given advice to FEP on compliance with PECR.
2. FEP may obtain a commercial advantage over its competitors by generating leads from unlawful marketing practices.
3. FEP did not identify the person who was sending or instigating the automated marketing calls, or provide the address of the person or a telephone number on which this person can be reached free of charge.

Mitigating Factors:

1. There is a potential for damage to FEP's reputation which may affect future business.

Remedial Action:

No mention of remedial action.

Direct Choice Home Improvements Ltd ("Direct Choice")

21 March 2016

£50,000

PECR – Regulation 21

Direct Choice is a company that provides and installs home improvement products such as doors, windows, conservatories, kitchens and bathrooms.

Between 29 April 2015 and 29 September 2015, 167 complaints were made about unsolicited direct marketing calls to the TPS and the ICO. TPS contacted Direct Choice to give it a chance to provide an explanation. However, Direct Choice did not respond to communications from the TPS on multiple occasions. On other occasions, Direct Choice relied on the explanation that it purchased its marketing list from a third party, without verifying the list on its own. The ICO found that repeat calls were made to subscribers who had asked for their number to be suppressed. Also, Direct Choice was in the top 20 list of companies about which the TPS received the most complaints on several occasions.

Aggravating Factors:

1. Direct Choice may obtain a commercial advantage over its competitors by generating leads from unlawful marketing practices.
2. There was a failure to fully cooperate with the ICO.

Mitigating Factors:

1. There is a potential for damage to Direct Choice's reputation which may affect future business.

Remedial Action:

No mention of remedial action.

Total value of breaches issued per type of legislation in 2016:

Breach of DPA 1st & 2nd principles: ***£43,000***

Breach of DPA 7th principle: ***£1,150,500***

Breach of PECR Regulation 19: ***£1,320,00***

Breach of PECR Regulation 21: ***£180,000***

Breach of PECR Regulation 22: ***£480,000***

Breach of PECR Regulations 22 & 23: ***£70,000***

Breach of PECR Regulation 5A: ***£2,000***

Falcon & Pointer Limited

21 March 2016

£175,000

PECR – Regulation 19

Falcon & Pointer Limited is a claims management company offering payment protection insurance and packaged bank accounts. Between 26 June 2015 and 31 October 2015, the ICO received 5,535 complaints about automated direct marketing calls made by the company. The ICO contacted Falcon & Pointer Limited to remind it of its obligations under the PECR, and requested evidence of prior consent from recipients of the automated marketing calls. Falcon & Pointer Limited claimed that the data was screened against the TPS or was "opt-in", but failed to produce evidence to support its claims. Falcon & Pointer Limited informed the ICO that it ceased making automated calls by the end of June 2015, but the ICO continued to receive complaints. The ICO established that Falcon & Pointer Limited made a further 2,475,481 calls between 26 June 2015 and 7 September 2015.

Aggravating Factors:

1. Falcon & Pointer Limited may obtain a commercial advantage over its competitors by generating leads from unlawful marketing practices.
2. Falcon & Pointer Limited did not identify the person who was sending or instigating the automated marketing calls, or provide the address of the person or a telephone number on which this person can be reached free of charge in breach of PECR Regulation 14.

Mitigating Factors:

1. There is a potential for damage to Falcon & Pointer Limited's reputation which may affect future business.

Remedial Action:

No mention of remedial action.

TalkTalk Telecom Group Plc ("TalkTalk")

24 March 2016

£1,000

PECR – Regulation 5A

TalkTalk is a telecommunications company. TalkTalk failed to notify the ICO within 24 hours of a personal data breach that occurred on 16 November 2015. A bug in the customer password reset facility allowed a customer to access the name, address, telephone and account billing information of another customer. On 18 November 2015, the affected customer contacted TalkTalk regarding this incident. However, TalkTalk did not notify the ICO until 1 December 2015.

This notification is mandatory under Regulation 5A of the PECR. The Commissioner was satisfied that the evidence provided by the customer was sufficient to enable TalkTalk to conclude that a security incident had occurred.

Fixed monetary penalty under PECR Section 5C.

Aggravating Factors:

No mention of aggravating factors.

Mitigating Factors:

No mention of mitigating factors.

Advice Direct Ltd trading as National Workers Office ("Advice Direct")

30 March 2016

£20,000

PECR – Regulation 21

Advice Direct Ltd is a company whose business involves calling individual subscribers with a view to generating leads for potential claims for damages in respect of hearing loss caused by working in a noisy environment. Between 7 April 2015 and 31 July 2015, the ICO received 57 complaints about Advice Direct via the ICO's online reporting tool from subscribers who were registered with the TPS. The TPS received 160 complaints about Advice Direct.

Many of the subscribers complained that they received multiple calls on the same day, and the callers were abusive and threatening. False and misleading statements were also made about records held by Advice Direct, which indicated that household members had worked in a noisy environment. Some of the callers gave the false impression that Advice Direct was offering a government-backed scheme.

The ICO held that the contravention was negligent as Advice Direct should have been aware of its responsibilities in this area.

Aggravating Factors:

1. Advice Direct may obtain a commercial advantage over its competitors by generating leads from unlawful marketing practices.

Mitigating Factors:

1. There is a potential for damage to tAdvice Direct's reputation which may affect future business.

Remedial Action:

No mention of remedial action.

EE Limited

20 April 2016

£1,000

PECR – Regulation 5A

EE Limited is a British Mobile network operator, internet service provider and a subsidiary of BT Group. EE Limited failed to notify the ICO within 24 hours of a personal data breach notified to it on 14 January 2016. On that day, EE Limited received a telephone call from a customer who believed that he may have been the victim of identity fraud. Someone purporting to be the customer had telephoned EE Limited previously and was provided with his account password, in violation of security procedures. However, EE Limited did not notify the ICO until 18 January 2016.

No aggravating or mitigating factors as fixed monetary penalty under PECR Regulation 5C.

Remedial Action:

No mention of remedial action.

Total number of MPNs per year:

2016: ***35***
2015: ***18***
2014: ***11***
2013: ***18***
2012: ***25***

Chief Constable of Kent Police

18 April 2016

£80,000

DPA – 7th Principle

Kent Police sent all files in a subject's mobile phone to an officer's solicitor by mistake, because of inappropriate security measures. The subject had accused the officer, who was her partner, of domestic abuse. She had submitted her mobile phone containing a video recording as evidence, and Kent Police had extracted the entire contents of the mobile phone onto CDs. Though she later changed her mind about pursuing the complaint, the officer was the subject of a misconduct investigation. A manager from Kent Police sent the complete contents of the phone, which included details of the data subject's divorce, texts and intimate photographs, to the officer's solicitor by mistake.

The ICO found that the Kent Police did not have in place appropriate organisational measures for ensuring so far as possible that such incidents would not occur.

Aggravating Factors:

The data subject made a formal complaint to Kent Police.

Mitigating Factors:

1. Kent Police made prompt efforts to secure the return of the full working copy. However, those efforts are the bare minimum to be expected of any data controller in such circumstances, and those efforts have in this case been unsuccessful, resulting in ongoing distress to the data subject.
2. Kent Police acted promptly to ensure that, in future, administrative staff members are not given full responsibility for such disclosure procedures.
3. Kent Police referred this incident to the ICO itself and was co-operative during the ICO investigation.
4. A monetary penalty may have a significant impact on Kent Police's reputation.

Remedial Action:

1. Kent Police has ensured that, in future, administrative staff members are not given full responsibility for such disclosure procedures.

Nevis Home Improvements Ltd

25 April 2016

£50,000

PECR – Regulation 19

Nevis Home Improvements Ltd sells products that improve energy efficiency. Over a five month period, Nevis Home Improvements Ltd sent or instigated 1,538,682 automated marketing calls to subscribers without their prior consent. Between 21 May and 27 August 2015, the ICO office received 175 complaints via the online reporting tool and the TPS received 8 complaints. A number of automated marketing calls had been received by subscribers in relation to Nevis Home Improvements Ltd's products. The calls did not identify the sender and the option of speaking to a person or suppressing the number was not always effective.

The ICO contacted Nevis Home Improvements Ltd to remind the organisation of its obligations under the PECR, and requested Nevis Home Improvements Ltd to provide evidence that it had obtained prior consent from recipients of these calls. The Company informed the ICO that it had purchased "opt-in" data from a reputable supplier and screened the data against the TPS list. However, Nevis Home Improvements Ltd failed to produce any evidence that it had the prior consent of the recipients to send or instigate the calls.

The ICO noted that organisations buying marketing lists from third parties, or contracting with third parties to carry out marketing, must make rigorous checks to ensure that the data was obtained fairly and lawfully, with the recipient's consent. If using the list for automated marketing calls, organisations should take extra care. Contractual assurances are not sufficient due diligence.

The ICO held that the contravention was negligent as Nevis Home Improvements Ltd should have been aware of its responsibilities in this area.

Aggravating Factors:

1. Nevis Home Improvements Ltd attempted to send or instigate a further 991,867 automated marketing calls during the period of complaint that were not connected.
2. Nevis Home Improvements Ltd may obtain a commercial advantage over its competitors by generating leads from unlawful marketing practices.
3. Nevis Home Improvements Ltd did not identify the person who was sending or instigating the automated marketing calls and provide the address of the person or a telephone number on which he can be reached free of charge in breach of PECR Regulation 24.

Mitigating Factors:

1. Nevis Home Improvements Ltd has confirmed that it will not be running a similar marketing campaign.
2. There is a potential for damage to Nevis Home Improvements Ltd's reputation which may affect future business.

Remedial Action:

No mention of remedial action.

Blackpool Teaching Hospitals NHS Foundation Trust ("Trust")

28 April 2016

£185,000

DPA - 7th Principle

The Trust was required to publish annual equality and diversity metrics on its external website. On 28 February 2014, the equality and diversity lead in HR asked the electronic staff records team (Team) for the equality and diversity metrics held on the electronic staff records system (ESR). The Team sent the spreadsheets to the equality and diversity lead on 3 March 2014. The Team had not detached the associated data because it was not aware that Excel had this feature within pivot tables. The equality and diversity lead then forwarded the spreadsheets to the web services team asking it to upload them to the Trust's website. The web services team uploaded the spreadsheets and the associated data was inadvertently published on the Trust's website on 4 March 2014.

On 30 January 2015, the Team received a similar request for metrics. A member of the Team searched the Trust's website to check the format of the Excel spreadsheets from previous years to ensure consistent replication. The individual inadvertently double-clicked on a pivot table on the 'leavers' spreadsheet which opened up the associated data and enabled access to data about protected groups and equality pay bands. The spreadsheets contained confidential and sensitive personal data relating to 6,574 past and present employees including their name, pay scale, National Insurance number and date of birth. It also contained their disability status, ethnicity, religious belief and sexual orientation and had been publicly available on the Trust's website for the past 11 months. During this time, the pivot tables were accessed at least 59 times by 20 visitors, and on several occasions the associated data was downloaded by persons unknown.

The ICO noted that the contravention was not deliberate. However he did conclude that the inadequacies which caused the contravention were a serious oversight and that the Trust knew or ought reasonably to have known that there was a risk that the contravention might occur.

Aggravating Factors:

1. The Trust was not aware of the security breach for 11 months.
2. There was a delay in the cached data being removed from the search engines.
3. The data subjects were not notified about the security breach until early May 2015.
4. The ICO received a complaint from a data subject.
5. The Trust received requests from 240 of the data subjects to see the information that had been compromised.

Mitigating Factors:

1. The Trust conducted a full investigation.
2. The Trust took remedial action.
3. The Trust reported this incident to the ICO and was cooperative during the investigation.
4. A monetary penalty may have had a significant impact on the Trust's reputation and, to an extent, its resources.

Remedial Action:

The Trust took remedial action.

Total value of MNPs per year

2016: ***£3,245,500***
2015: ***£2,031,250***
2014: ***£1,152,500***
2013: ***£1,520,000***
2012: ***£2,430,000***
2011: ***£541,000***

Chelsea and Westminster Hospital NHS Foundation Trust ("Trust")

9 May 2016

£180,000

DPA – 7th Principle

56 Dean Street (Soho) is a clinic within the Trust that provides sexual health and HIV services to patients. The clinic developed a service (**Option E**) to enable patients with HIV to receive results and make appointments/enquiries by e-mail. Patients of Option E, in addition to a small number without HIV, received clinic newsletters.. In March 2010, a member of staff in the Trust's Pharmacy Department sent a questionnaire to 17 patients in relation to their access to HIV treatment. The e-mail addresses were entered into the "to" field instead of the blind carbon copy ("bcc") field enabling recipients of the email to see the e-mail addresses of all recipients. Following this security breach, the Trust implemented some remedial measures. However, these measures did not include specific training to remind staff to double check that group e-mail addresses were entered into the correct field. Additionally, these measures did not include replacing the e-mail account used with an account with a function enabling a separate e-mail to be sent to each service user on the distribution list. On 1 September 2015, a member of staff in the clinic sent a newsletter to the 781 subscribers of Option E. The e-mail addresses were entered into the "to" field instead of the "bcc" field in error enabling recipients of the e-mail to see the e-mail addresses of all recipients. Of these 781 email addresses, 730 contained the full names of service users.

The ICO notes that the contravention was not deliberate but held that the Trust ought reasonably to have known that the group email addresses would be vulnerable to a security breach in the absence of appropriate technical and organisational measures.

Aggravating Factors:

1. The Trust received 15 complaints from the affected individuals.
2. The ICO received 9 complaints from affected individuals.
3. The clinic did not inform the service users when they subscribed to option E that their email addresses would be used to send newsletters to other service users by bulk mail.
4. One of these email addresses should have been removed from the e-mail distribution list for Option E as they had re-located.

Mitigating Factors:

1. The Trust was fully co-operative with the ICO.
2. The Trust apologised to the affected individuals.
3. The Trust took substantial remedial action.
4. There would have been a significant impact on the Trust's reputation as a result of this security breach.

Remedial Action:

The Trust took substantial remedial action.

Better for the Country Ltd

9 May 2016

£50,000

PECR – Regulation 22

Better for the Country Ltd campaigned for the UK to leave the European Union, formerly under the name 'The Know' and subsequently as 'Leave.EU'. Unsolicited directed marketing text messages were sent as part of the campaign. Between 1 May and 7 October 2015, 134 complaints were made through GSMA's Spam Reporting Service about the receipt of unsolicited direct marketing text messages sent by Better for the Country Ltd. In the same period, 6 complaints were made directly to the ICO. The ICO warned Better for the Country Ltd of the monetary penalties it could face for a PECR breach. In response Better for the Country Ltd stated that the messages were sent to registered supporters and individuals whose data had been received from a third party who had obtained the individuals' consent to receipt of marketing messages. The ICO determined that the consent received by the third party was not valid. Better for the Country Ltd stated that it had sent a total of 501,135 text messages between 1 May and 7 October 2015 to individuals whose details had been obtained from a third party supplier.

The ICO held that the contraventions were negligent. In particular, the ICO noted that Better for the Country Ltd did not undertake sufficient due diligence with regard to its third party data supplier.

Aggravating Factors:

No mention of aggravating factors

Mitigating Factors:

1. Better for the Country Ltd fully co-operated with the ICO's investigation.
2. There was a potential for damage to Better for the Country Ltd's reputation.

Remedial Action:

No mention of remedial action.

12 Number of MPNS issued in 2016 with value over £100,000

Check Point Claims Ltd ("CPCL")

11 May 2016

£250,000

PECR – Regulation 19

In June 2015, the ICO identified that a number of complaints had been received about the receipt of automated marketing calls relating to hearing loss claims. The recorded message did not identify the sender or instigator of the call. On investigation it was determined some of the calls could be traced to Check Point Claims Ltd (CPCL). The relevant communications service provider confirmed that CPCL sent or instigated 17,565,690 automated marketing calls between 30 March and 30 September 2015; these calls were connected to approximately 6,388,122 subscribers.

During this period, the ICO received 248 complaints about automated marketing calls made from the CPCL's allocated to CPCL and the TPS also received 50 complaints about CPCL. The essence of the complaints was that the calls were at inconvenient times such as evenings and weekends, often repeatedly and that the receiver of the call had not worked in a noisy environment as claimed in the recorded message.

The ICO concluded that CPCL deliberately contravened Regulation 19.

Aggravating Factors:

1. CPCL attempted to send or instigate a further 11,177,568 automated marketing calls during the period of complaint that were not connected.
2. CPCL may have obtained a commercial advantage over its competitors by generating leads from unlawful marketing practices.
3. The ICO noted that CPCL had contravened PECR Regulation 24 in that it did not identify the person who was sending on instigating the automated marketing calls and provide the address of the persona or a telephone number on which he could be reached free of charge.

Mitigating Factors:

1. CPCL confirmed that it would not run a similar marketing campaign.
2. CPCL co-operated with the ICO's investigation.
3. The potential reputational damage which could affect future business.

Remedial Action:

No mention of remedial action.

Chief Constable of Dyfed-Powys Police

2 June 2016

£150,000

DPA – 7th Principle

A police officer sent an email containing a list of eight individuals intended for five internal recipients to an unauthorised, external recipient, a community scheme member. She could infer that the individuals on the list were sex offenders. The officer selected the unauthorised recipient's address accidentally by accessing the global address book. The ICO found that Dyfed-Powys Police did not have in place appropriate technical and organisational measures to ensure that such an incident could not occur. In particular, Dyfed-Powys Police failed to ensure that the global address book only contained internal e-mail addresses, that an internal e-mail address was always the first entry in the global address book and failed to give officers specific guidance or training on the importance of double checking that an email address is correct before information is sent out.

The ICO concluded that the contravention was not deliberate but that the Police knew or ought reasonably to have known that there was a risk that this contravention would occur. The Police force was used to sending internal and external e-mails containing confidential and sensitive personal data on a daily basis and ought reasonably to have been aware that it needed to ensure in so far as possible that the email was sent only to the intended recipients.

Aggravating factors:

Dyfed-Powys Police did not take any remedial action until six e-mails containing personal data had been sent to the community scheme member in error.

Mitigating factors:

1. The e-mail was deleted and the information had not been further disseminated as far as the ICO is aware.
2. Dyfed-Powys Police reported this incident to the ICO and were co-operative during this investigation.
3. Dyfed-Powys Police took substantial remedial action.
4. The affected data subjects were notified about the incident.
5. A monetary penalty would have had a significant impact on Dyfed-Powys Police's reputation.

Remedial Action:

Dyfed-Powys Police took substantial remedial action

Quigley & Carter Limited

6 June 2016

£80,000

PECR – Regulation 22

Quigley & Carter Limited - a claims management company - offers services in respect of mis-sold packaged bank accounts via its website www.mybankrefund.com. Between 6 April and 9 June 2015, 2,620 complaints were made through GSMA's Spam Reporting Service as a result of unsolicited direct marketing text messages sent by Quigley & Carter Limited. In the same period 69 complaints were made directly to the ICO. Quigley & Carter Limited reported that it had contracted with a third party to send the unsolicited text messages on its behalf. However, Quigley & Carter Limited was unable to provide any evidence that the recipients of the text messages had provided consent.

The ICO considered that the contravention was deliberate.

He also concluded that it was negligent, emphasising that organisations buying marketing lists from third parties, or contracting with third parties, to carry out marketing for them, must make rigorous checks to satisfy themselves that the third party has obtained the personal data that it is using fairly and lawfully, and that they have the necessary consent. It is not acceptable to rely on assurances of indirect consent without undertaking proper due diligence.

Aggravating factors:

1. Quigley & Carter Limited may have obtained a commercial advantage over its competitors by generating leads from unlawful marketing practices.

Mitigating factors:

1. The potential reputational damage which could affect future business.

Remedial Action:

No mention of remedial action.

Advanced VoIP Solutions Ltd

7 June 2016

£180,000

PECR – Regulation 19

The ICO fined Advanced VoIP Solutions Ltd that instigated automated nuisance calls. Between January and October 2015, the ICO received 6,381 complaints through its online reporting tool relating to repeated automated marketing calls being received by Advanced VoIP Solutions Ltd's subscribers in relation to personal protection insurance, packaged bank accounts and flight delays from Advanced VoIP Solutions Ltd without the subscriber's prior consent. Subscribers were then charged if they dialled back to attempt to speak to a person or identify who had sent the automated marketing call.

The contravention was held to be deliberate by the ICO.

Aggravating factors:

1. The use of "added value" numbers caused some subscribers to suffer financial loss.
2. The ICO continued to receive similar complaints after October 2015.
3. Advanced VoIP Solutions Ltd may have obtained a commercial advantage over its competitors by generating leads from unlawful marketing practices.
4. Advanced VoIP Solutions Ltd contravened PECR Regulation 24 in that it did not identify the person who was sending or instigating the automated marketing calls and provide the address of the person or a telephone number on which he can be reached free of charge.

Mitigating factors:

1. The potential reputational damage which could affect future business.

Remedial Action:

No mention of remedial action.

Regal Chambers Surgery

8 August 2016

£40,000

DPA – 7th Principle

A GP practice revealed confidential details about a woman and her family to her estranged ex-partner.

Mr A was acrimoniously divorced from the mother of his 5 year old son ("Child B"). In January 2013, child B's mother warned the Practice of the family's problems and specifically asked the Practice not to inform Mr A of their whereabouts. This information was placed on Child B's medical record. When Mr A made a Subject Access Request to the GP Practice, it sent all of Child B's medical record to Mr A, only four days after receiving the request.

The Commissioner concluded that the contravention was not deliberate but that the practice knew or ought reasonably to have known that this contravention would occur. The ICO held that the practice should have been aware that there was a risk unless it ensured the process was governed by adequate written procedures, undertaken by staff with appropriate experience and supervision and checked the material physically prior to disclosure.

Aggravating factors:

1. Child B's mother has made a complaint to the ICO.

Mitigating factors:

1. The Practice acted promptly to ensure that, in future, staff members are not given full responsibility for disclosure procedures.
2. The Practice referred this incident to the ICO itself and was co-operative during the investigation.
3. A monetary penalty may have a significant impact on the Practice's reputation.

Remedial Action:

Remedial action has been taken.

Hampshire County Council

10 August 2016

£100,000

DPA – 7th Principle

Hampshire County Council has been hit with a £100,000 fine by the ICO after documents containing personal details of over 100 people were found in a building it vacated.

The ICO held that the contravention was not deliberate but that the Council knew or ought reasonably to have known that there was a risk that the contravention would occur. The decommissioning process should have been governed by an adequate written procedure.

Aggravating factors:

There were no aggravating factors.

Mitigating factors:

1. The information was recovered from the building it vacated.
2. The Council has taken remedial action.
3. The Council referred this incident to the ICO itself and was co-operative during the ICO's investigation.
4. A monetary penalty may have a significant impact on the Council's reputation and (to an extent) on its resources.

Remedial Action:

The Council has taken remedial action.

£1,214,250

Increase of total value of MPNs in 2016 versus 2015

Whitehead Private Nursing Home Ltd

15 August 2016

£15,000

DPA – 7th Principle

A nursing home in County Antrim has been fined £15,000 for breaking the law by not looking after the sensitive personal details in its care. An unencrypted laptop holding confidential and sensitive personal data was taken home and then stolen in a burglary.

The contravention was not deliberate but the nursing home knew or ought reasonably to have known that there was a risk that this contravention would occur. The laptop should have been technically and/or physically protected.

Aggravating factors:

There were no aggravating factors.

Mitigating factors:

1. The laptop was password protected.
2. The information has not been further disseminated as far as the ICO is aware.
3. The data subjects were notified about the security breach.
4. This incident was reported to the ICO.
5. Substantial remedial action has now been taken.
6. A monetary penalty may have a significant impact on the nursing home's reputation and (to an extent) on its resources.

Remedial Action:

Substantial remedial action has now been taken.

Omega Marketing Services Ltd

5 September 2016

£60,000

PECR – Regulation 21

A solar panels and green energy equipment company - Omega Marketing Services Ltd – was fined by the ICO for making 1.6 million nuisance calls to try and sell solar panels and green energy equipment.

The ICO held that the contravention was not deliberate but was negligent. Omega Marketing Services Ltd should have carried out due diligence checks, screened the data against the TPS register/ its own suppression list and providing the company's telesales staff with written procedures and training regarding PECR.

Aggravating factors:

1. Omega Marketing Services Ltd may obtain a commercial advantage over its competitors by generating leads from unlawful marketing practices.
2. Omega Marketing Services Ltd did not identify the person who was sending or instigating the marketing call and, if requested, provide the address of the persona or a telephone number on which he can be reached free of charge in breach of PECR Regulation 4.

Mitigating factors:

1. There is a potential for damage to the Omega Marketing Services Ltd's reputation which may affect future business.

Remedial Action:

No mention of remedial action.

Vincent Bond & Co Limited

5 September 2016

£40,000

PECR – Regulation 22

Vincent Bond & Co Limited - a debt management company – was fined for sending unwanted marketing texts.

The ICO held that the contravention was not deliberate but the company knew or ought reasonably to have known that there was a risk that the contravention would occur, given that the issue of unsolicited text messages has been widely publicised by the media. The ICO pointed out that the guidance states that organisations can generally only send marketing texts to individuals if that person has specifically consented to receiving them.

Aggravating factors:

1. Vincent Bond & Co Limited may obtain a commercial advantage over its competitors by generating leads from unlawful marketing practices.

Mitigating factors:

1. Vincent Bond & Co Limited has taken substantial remedial action.
2. There is a potential for damage to Vincent Bond & Co Limited's reputation which may affect future business.

Remedial Action:

No mention of remedial action.

Carfinance247 Limited

12 September 2016

£30,000

PECR – Regulation 22

Carfinance247 Limited - a car finance brokerage company - used a public telecommunications service for the purpose of instigating 65,000 unsolicited direct marketing text messages.

Aggravating factors:

1. Carfinance247 Limited may obtain a commercial advantage over its competitors by generating leads from unlawful marketing practices
2. The company did not identify the person who was sending or instigating direct marketing text messages or provide a valid address to which the recipient of the communication may send a request that such communications cease in breach of PECR Regulation 23

Mitigating factors:

1. There is a potential for damage to the Carfinance247 Limited's reputation which may affect future business.

Remedial Action:

No mention of remedial action.

7 Increase of total number of MPNs in 2016 versus 2015

Intelligent Lending Limited t/a Ocean Finance

27 September 2016

£130,000

PECR – Regulation 22

Intelligent Lending Limited - a broker of a number of credit related products - used a public telecommunications service for the purpose of instigating 4,531,824 unsolicited direct marketing text messages.

The ICO held that the contraventions were not deliberate but were negligent. The ICO stated that organisations buying marketing lists from third parties or contracting with third parties to carry out marketing for them must make rigorous checks to satisfy themselves that the third party has obtained the data that it is using fairly and lawfully and that they have the necessary consent. The ICO states that it is not acceptable to rely on assurances of indirect consent without undertaking proper due diligence and provides a checklist to follow.

Aggravating factors:

1. A proportion of the text messages were sent to individuals on more than one occasion.

Mitigating factors:

1. Intelligent Lending Limited fully co-operated with the ICO's investigation.
2. There is a potential for damage to the Intelligent Lending Limited's reputation which may affect future business.
3. Intelligent Lending Limited had attempted to conduct appropriate due diligence albeit this was found by the ICO to be ultimately ineffectual.

Remedial Action:

No mention of remedial action.

TalkTalk Telecom Group PLC

30 September 2016

£400,000

DPA – 7th Principle

Telecommunications company TalkTalk was issued a record £400,000 fine by the ICO for security failings that allowed a cyber attacker to access customer data "with ease". The Group had not been aware that the infrastructure of Tiscali, which it acquired in 2009, included webpages that were still available via the internet in 2015, with access to an underlying Tiscali database.

The ICO held that the contravention was not deliberate but that the Group knew or ought to have reasonably known that there was a risk that this contravention would occur. The Group should have been aware of the Tiscali infrastructure and of the SQL injection security vulnerability.

Aggravating factors:

There were no aggravating factors.

Mitigating factors:

1. The database was subjected to a criminal attack.
2. TalkTalk reported this incident to the ICO and was cooperative during the ICO's investigation.
3. TalkTalk notified all of its customers and offered 12 months of free credit monitoring.
4. TalkTalk has taken substantial remedial action.
5. A monetary penalty may have a significant impact on TalkTalk's reputation.
6. This incident has been widely publicised in the media.

Remedial Action:

TalkTalk has taken substantial remedial action.

Rainbow (UK) Limited

10 October 2016

£20,000

PECR – Regulation 22

Rainbow (UK) Limited was fined for sending thousands of spam texts about loans.

The ICO held that the contravention was not deliberate but was negligent. Rainbow (UK) Limited relied upon contractual assurances from its third party data supplier that the necessary consent had been obtained for sending unsolicited direct marketing text messages and did not undertake sufficient due diligence.

Aggravating factors:

1. The scale of the contravention could have been considerably larger as Rainbow (UK) Limited had attempted to send 580,302 direct marketing text messages. The ICO considers this to be a significant aggravating factor.
2. Some of the text messages were sent at unsocial hours.

Mitigating factors:

1. Rainbow (UK) Limited co-operated with the ICO's investigation.
2. There is a potential for damage to Rainbow (UK) Limited's reputation which may affect future business.

Remedial Action:

No mention of remedial action.

Nouveau Finance Ltd

7 November 2016

£70,000

PECR – Regulations 22

Nouveau Finance Ltd was fined £70,000 for sending 2.2 million marketing text messages, without the recipients' consent to do so.

Nouveau Finance is a leads generator providing a loan matching service for individuals. In part, it generates leads for its business by instigating the sending of direct text messages directing individuals to websites owned by the, for example: "Lisa, are you in a tight spot? Make a simple application for Emergency funds! Visit www.txtcash.co/2cZ5o to get started. Reply STOP 2 end".

Between 1 August 2015 and 10 January 2016, 92 complaints were made to the GSMA's Spam Reporting Service about the receipt of unsolicited direct marketing text messages from Nouveau Finance.

The ICO held that the contravention was not deliberate but was negligent. Nouveau Finance Ltd was unable to provide any evidence that it had undertaken due diligence and therefore failed to take reasonable steps to prevent the contraventions.

Aggravating factors:

1. Nouveau Finance Ltd may have obtained a commercial advantage over its competitors by generating leads from unlawful marketing practices.
2. Nouveau Finance Ltd did not identify the person who was sending or instigating direct marketing text messages or provide a valid address to which the recipient of the communication may send a request that such communications cease has not been provided in breach of PECR Regulation 23.

Mitigating factors:

1. There is a potential for damage to the Nouveau Finance Ltd's reputation which may affect future business.

Remedial Action:

No mention of remedial action.

Assist Law Limited ("Assist Law")

3 November 2016

£30,000

PECR – Regulation 21

Assist Law, based in Weston-super-Mare, Somerset, made unsolicited marketing calls to people registered with the TPS, without consent to do so for over a year.

The ICO held that the contraventions were not deliberate but were negligent. Assist Law had been aware of its obligations under PECR since at least May 2015 when it was first contacted by the ICO and provided with advice on its obligations under PECR. The fact that Assist Law knew that people were complaining about calls they were receiving shows that the company ought to have known the risk of contravening PECR. The TPS also contacted Assist Law on each occasion a complaint was made to it which should have also made the company aware of the risk.

Aggravating factors:

There were no aggravating factors.

Mitigating factors:

1. In setting the level of the fine, the ICO noted that there was a potential for damage to Law Assist's reputation which may affect future business.

Remedial Action:

No mention of remedial action.

The Historical Society (an unincorporated association)

7 November 2016

£500

DPA – 7th Principle

The Historical Society was fined after a laptop containing sensitive personal data was stolen whilst a member of staff was working away from the office. The laptop, which was not encrypted, contained the details of people who had donated artefacts to the society.

The ICO held that the contravention was not deliberate but that the Historical Society knew or ought reasonably to have known that there was a risk that this contravention would occur. There was no good reason for the officer not having been issued with an encrypted laptop and for the absence of policies governing the use of encryption, homeworking and the storage of mobile devices.

Aggravating factors:

There were no aggravating factors.

Mitigating factors:

1. The location (undisclosed) in which the Historical Society's officer left the laptop
2. The laptop was password protected.
3. The information has not been further disseminated as far as the ICO is aware.
4. A monetary penalty may have a significant impact on the Historical Society's reputation.

Remedial Action:

No mention of remedial action.

Silver City Tech Limited

25 November 2016

£100,000

PECR – Regulation 22

Silver City Tech Limited was once of two companies found responsible for sending millions of spam texts offering easy access to loans.

Separate ICO investigations into Dorset-based Silver City Tech Ltd and Oracle Insurance Brokers Ltd, in London, found the firms had broken the law because they did not have the consent of the people the text messages were sent to.

The ICO held that the contraventions were not deliberate but were negligent. The ICO found that Silver City Tech Limited was unable to provide evidence that it had undertaken appropriate due diligence before the text messages were sent. The evidence of consent Silver City Tech Limited produced was inadequate; subscribers would not have anticipated that they would be the recipients of SMS marketing from Silver City Tech Limited.

Aggravating factors:

1. Silver City Tech Limited may obtain a commercial advantage over its competitors by generating leads from unlawful marketing practices.
2. After the ICO first contacted Silver City Tech Limited to advise it of the complaints received, the unsolicited marketing text messages continued to be sent. A further 1,942,182 messages were sent during the period 18 December 2015 and 16 April 2016.
3. Silver City Tech Limited accepted that in some cases duplicate messages were sent to the same individual.

Mitigating factors:

1. There is a potential for damage to the Silver City Tech Limited's reputation which may affect future business.

Remedial Action:

No mention of remedial action.

Oracle Insurance Brokers Limited

25 November 2016

£30,000

PECR – Regulation 22

Oracle Insurance Brokers Limited was one of two companies found responsible for sending millions of spam texts offering easy access to loans.

Separate ICO investigations revealed that Oracle Insurance Brokers Ltd, had broken the law because they did not have the consent of the people to whom the text messages were sent.

The ICO held that the contraventions were not deliberate but were negligent. Oracle Insurance Brokers Limited did not undertake sufficient due diligence. Had it carried out a proper review of the privacy notices of the websites from which the data had been obtained, it should have been clear that Oracle Insurance Brokers Limited did not have consent to instigate the sending of unsolicited direct marketing text messages.

Aggravating factors:

1. Oracle Insurance Brokers Limited may obtain a commercial advantage over its competitors by generating leads from unlawful marketing practices.

Mitigating factors:

1. There is a potential for damage to the Oracle Insurance Brokers Limited's reputation which may affect future business.

Remedial Action:

No mention of remedial action.

Royal Society for the Prevention of Cruelty to Animals

5 December 2016

£25,000

(ICO stated that the penalty imposed could have been significantly higher given the seriousness, nature and extent of the contraventions)

DPA – 1st & 2nd Principles

The Royal Society for the Prevention of Cruelty to Animals ("RSPCA") secretly screened millions of their donors so they could target them for more money, a comprehensive ICO investigation has found.

The ICO considered four issues in detail: the use of the member only "Reciprocate" data sharing scheme; the sharing of personal data despite opt-outs; the use of wealth management companies to conduct wealth analysis and the practices of data-matching and tele-matching.

The ICO found that the RSPCA's actions were deliberate in all but the second category (sharing despite opt-outs) where she held that the RSPCA should have known that there was a risk of a contravention.

Aggravating factors:

1. The RSPCA has followed the unlawful practices described above over a period of several years. Over such a time period and range of activity, an organisation with the size and resources of RSPCA should have detected and acted upon the deficiencies in its practices. This is indicative of an organisational failure to fulfil its data protection and privacy obligations.
2. The RSPCA's practices appear to have been driven by financial gain. The fact that it is a charity is not an excuse in this respect. In fact, the public is arguably entitled to expect charities to be especially vigilant in complying with their legal obligations.
3. The RSPCA has contravened the fundamental rights of millions of individuals to have their personal data processed in accordance with the DPA and Directive 95/46/EC. Many of those individuals are likely to have suffered more than one contravention.
4. By failing adequately to explain to data subjects how their personal data would be used, the RSPCA has deprived them of control and informed decision-making about their personal data to a significant extent.
5. The RSPCA's activities as described above have exposed the relevant data subjects to substantially distressing and/or damaging consequences, including: intrusions into their privacy due to increased direct marketing communications from the RSPCA and other charities. It is likely that many individuals will have been persuaded - by RSPCA and/or other charities - to increase their financial support. Those financial consequences will to a significant extent have flowed from the RSPCA's unlawful data protection practices.

Mitigating factors:

1. The RSPCA co-operated with the ICO's investigations and self-reported the contraventions concerning sharing personal data despite opt outs.
2. The RSPCA is a charity that seeks to further its objectives in the public interest, rather than for purely private interests or mere financial gain.
3. The RSPCA may have been ignorant that the practices which were the subject of the monetary penalty contravened the DPA, i.e. it did not set out to break the law, act maliciously or cause damage or distress.
4. The RSPCA is likely to take remedial action. It has an interest in ensuring that it complies with the law, retains the confidence of its donors and the public and does not suffer reputational damage.
5. The RSPCA's practices may to an extent have reflected commonplace - albeit mistaken and unlawful - approaches in the charitable sector.
6. The monetary penalty may also have negative reputational consequences.

Remedial Action:

The RSPCA is likely to take remedial action.

British Heart Foundation

5 December 2016

£18,000

(ICO stated that the penalty imposed could have been significantly higher given the seriousness, nature and extent of the contraventions)

DPA – 1st & 2nd Principles

British Heart Foundation ("BHF") secretly screened millions of their donors so they could target them for more money, a comprehensive ICO investigation has found.

The ICO considered three specific issues: disclosure of personal data under the "Reciprocate" data sharing scheme; the use of wealth management companies to conduct wealth analysis and data matching and tele matching.

The ICO considered that the contraventions were deliberate.

Aggravating factors:

1. The BHF has followed the unlawful practices described above over a period of several years. Over such a time period and range of activity, an organisation with the size and resources of BHF should have detected and acted upon the deficiencies in its practices. This is indicative of an organisational failure to fulfil its data protection and privacy obligations.
2. The BHF's practices appear to have been driven by financial gain. The fact that it is a charity is not an excuse in this respect. In fact, the public is arguably entitled to expect charities to be especially vigilant in complying with their legal obligations.
3. The BHF has contravened the fundamental rights of millions of individuals to have their personal data processed in accordance with the DPA and Directive 95/46/EC. Many of those individuals are likely to have suffered more than one contravention.
4. By failing adequately to explain to data subjects how their personal data would be used, the BHF has deprived them of control and informed decision-making about their personal data to a significant extent.
5. The BHF's activities as described above have exposed the relevant data subjects to substantially distressing and/or damaging consequences, including: intrusions into their privacy due to increased direct marketing communications from the BHF and other charities. It is likely that many individuals will have been persuaded - by BHF and/or other charities - to increase their financial support. Those financial consequences will to a significant extent have flowed from the BHF's unlawful data protection practices.

Mitigating factors:

1. The BHF co-operated with the ICO's investigations.
2. The BHF is a charity that seeks to further its objectives in the public interest, rather than for purely private interests or mere financial gain.
3. The BHF may have been ignorant that the practices described above contravened the DPA, i.e. it did not set out to break the law, act maliciously or cause damage or distress.
4. The BHF has ceased the activities described in this notice.
5. The BHF's practices may to an extent have reflected commonplace - albeit mistaken and unlawful - approaches in the charitable sector.
6. The monetary penalty may have negative reputational consequences.

Remedial Action:

The BHF has ceased the activities described in the notice.

Prosecutions

Total	***16***

RFF Services (UK) Limited

21 January 2016

A building and plumbing company - RFF Services (UK) Limited - was prosecuted for failing to comply with an information notice issued by the ICO in relation to a subject access complaint from one of their former customers.

Action:

RFF Services (UK) Limited pleaded guilty, was fined £200, ordered to pay £425.95 costs and to pay a £20 victim surcharge.

I&K Prestige Food Limited (T/A Stokrotka)

18 March 2016

I&K Prestige Food Limited, which trades as Stokrotka and manufactures chilled and fresh convenience meals, was prosecuted for failing to notify the ICO of its data processing activities.

Action:

I&K Prestige Food Limited pleaded guilty, was fined £200,. ordered to pay £485.95 costs and to pay a £20 victim surcharge.

Keurboom Communications Limited

5 April 2016

Keurboom Communications Limited and its Director, Gregory Rudd, were prosecuted for failing to comply with a third party information notice issued by the ICO in relation to an ongoing investigation for PECR breaches.

Action:

Keurboom Communications Limited pleaded guilty, was fined £1500, ordered to pay £ 435.95 costs and to pay a £120 victim surcharge.

Mr Rudd was fined £1000, ordered to pay £435.95 costs and to pay a £100 victim surcharge.

David Barlow Lewis

7 April 2016

Former LV employee David Barlow Lewis was prosecuted for attempting to obtain personal data without the data controller's consent.

Action:

Mr Lewis was fined £300, ordered to pay £614.40 costs and to pay a £30 victim surcharge.

Getwork2day Ltd

22 April 2016

Getwork2day Ltd, a web based recruitment business, was prosecuted for failing to notify the ICO of its data processing activities.

Action:

Getwork2day Ltd was fined £500, ordered to pay £951.79 costs and to pay a £50 victim surcharge.

Mark Lloyd

26 May 2016

Mr Mark Lloyd was prosecuted at Telford Magistrates' Court for unlawfully obtaining data. Mr Lloyd, who worked at a waste management company in Shropshire, emailed the details of 957 clients to his personal email address as he was leaving to start a new role at a rival company. The documents contained personal information including the contact details of customers, as well as purchase history and commercially sensitive information.

Action:

Mr Lloyd pleaded guilty, was fined £300, ordered to pay £405.98 costs and to pay a £30 victim surcharge.

Total number of prosecutions per year

2016: **16**
2015: **11**
2014: **18**
2013: **7**
2012: **6**

Money Saving Champions Limited

7 June 2016

Money Saving Champions Limited was prosecuted for failing to notify the ICO of its data processing activities.

Action:

Money Saving Champions Limited pleaded guilty, was fined £350 and ordered to pay costs of £497.75.

Clarity Leeds Limited

21 July 2016

Clarity Leeds Limited was prosecuted at Barkingside Magistrates' Court for two offences of failing to comply with an Information Notice. The marketing company, about whom the ICO received a complaint from two individuals for non-compliance with subject access requests, were subsequently served with Information Notices to enable the ICO to make an assessment of the complaint and which the company failed to respond to.

Action:

Clarity Leeds Limited pleaded guilty, was fined £300, ordered to pay £489.85 costs and to pay a £20 victim surcharge.

Bizcall Communications Limited

18 August 2016

Bizcall Communications Limited was prosecuted at Birmingham Magistrates Court for failing to notify the ICO of its data processing activities.

Action:

Bizcall Communications Limited was found guilty, was fined £650, ordered to pay costs of £299.63 and to pay a victim surcharge of £65.

Triforce Recruitment Ltd

21 September 2016

Triforce Recruitment Ltd was prosecuted at Westminster Magistrates' Court for failing to notify the ICO of its data processing activities.

Action:

Triforce Recruitment Ltd was fined £5,000, ordered to pay costs of £489.85 and to pay a victim surcharge of £120.

Beverley Wooltorton

25 October 2016

Former administrative employee Beverley Wooltorton was prosecuted at Ipswich Magistrates' Court for accessing personal information without a business need to do so. She accessed the medical records of people that she knew, including estranged family members, whilst employed by Ipswich Hospital NHS Trust.

Action:

Ms Wooltorton pleaded guilty, was fined £650 and ordered to pay £638.60 prosecution costs and to pay a £30 victim surcharge.

Kayleigh Evans

28 October 2016

A former administrative employee of Solent NHS Trust, Kayleigh Evans, was prosecuted at West Hampshire Magistrates' Court for accessing the sensitive medical records of a former girlfriend of her partner, without the consent of the data controller. The unlawful accesses to the records were over a 10 month period.

Action:

Ms Evans pleaded guilty, was fined £400, ordered to pay £683.60 prosecution costs and to pay a £40 victim surcharge.

Karun Tandon

2 November 2016

Karun Tandon was prosecuted at Manchester Magistrates' Court for unlawfully obtaining and selling personal data. Karun Tandom, who worked at Lex Autolease Limited emailed personal data of 551 Lex Autolease customers, relating to road traffic accidents, from his former employer's computer system to his personal email address, which he then sold on to a third party as personal injury leads.

Action:

Mr Tandon pleaded guilty to two offences , was fined £500, ordered to pay prosecution costs £364 and to pay a £25 victim surcharge.

Lesley Severs and Kayleigh Billington

11 November 2016

Lesley Severs and Kayleigh Billington were prosecuted by Liverpool Magistrates' Court for obtaining information about policy holders and the road traffic accidents they had been involved in, from insurance companies.

At the time of the offences the defendants worked at a claims management company, UK Claims Organisation Ltd, based in Liverpool. It was the prosecution case that data originally obtained unlawfully from a car hire company was used by the employees of the claims management company as leads, to make blagging calls to insurance companies. In the calls the defendants used various guises and tried to obtain further information from the insurers, in order to be able to sell cases on to solicitors as personal injury claims.

Action:

Kayleigh Billington pleaded guilty to 8 offences, was fined £320, ordered to pay a contribution to costs of £250 and to pay a victim surcharge of £20.

Lesley Severs pleaded guilty to 5 offences, was fined £250, ordered to pay a contribution to costs of £400 and to pay a victim surcharge of £20.

Keketso Monnapula

2 December 2016

A former agency admin worker of Tees Esk & Wear Valleys NHS Foundation Trust, Keketso Monnapula, was prosecuted at Harrogate Magistrates' Court for accessing the sensitive medical records of people that she knew, such as old school friends and a family member, without the consent of the data controller.

Action:

Ms Monnapula pleaded guilty to the offence, was fined £45, ordered to pay costs of £405.98 and to pay a victim surcharge of £20.

Wainwrights Estate Agents Ltd

20 December 2016

Wainwrights Estate Agents Ltd was prosecuted at Ipswich Magistrates' Court for failing to comply with a third party Information Notice.

Wainwrights Estate Agents Ltd, whom the ICO received a complaint from an individual for non-compliance with a subject access request, were subsequently served with an Information Notice to enable the ICO to make an assessment of the complaint and which the company failed to respond to.

Action:

Wainwrights Estate Agents Ltd pleaded guilty to the offence, was fined £250, ordered to pay a victim surcharge of £30 and to pay costs of £500.

Undertakings

Private sector	***10***
Public sector	***20***
Total	***30***

South West Yorkshire Partnership NHS Foundation Trust

4 January 2016

DPA – 7th Principle

This Trust experienced various breaches in data security such as disclosing a discharge letter to an unrelated third party, and upon further investigation two discharge letters were discovered within the same envelope. Further incidents such as sending letters to the wrong addresses, and addresses being incorrectly recorded had also occurred.

A follow up has been completed to provide an assurance that South West Yorkshire Partnership NHS Trust has appropriately addressed the actions agreed in its undertaking signed May 2015.

Undertakings signed in May 2015:

1. The 'Safe Haven Policy' is updated by the data controller in order to provide guidance on checking the contents of all correspondence sent.
2. Guidance on checking contact details is formalised into an appropriate policy.
3. All security incidents involving personal data are thoroughly investigated, with remedial actions and measures implemented within a timeframe for completion.
4. All appropriate measures should be taken by the data controller to protect personal data against unauthorised and unlawful processing, accidental loss, destruction, and/or damage.

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

1. 'The Safe Haven Policy' was updated in September 2015, with it due to have been ratified in October 2015.
2. Work had begun on creating processes to complement the updated validation check procedure guidance where incidents occurred. The Trust planned to implement periodic 'spot checks' to be performed by the Information Governance (IG) team.
3. The Trust amended the Datix incident reporting form in order to help staff identify and report IG incidents. This went live on 1 September 2015 and further work had begun to create a flowchart to assist incident reporting.
4. The Trust was planning to communicate all reported IG incidents to all staff, rather than those merely at a local level.
5. A 'Think Information Governance' campaign was launched to increase awareness of IG practices.
6. The Trust developed classroom-based IG training with increased relevance for staff, alongside specific e-learning modules.
7. The Trust should take further steps:
    a. Ensure the updated 'Safe Haven Policy' is ratified and made available to staff.
    b. Ensure local processes to check the content of correspondence are developed in all Trust areas.
    c. Review the Investigating and Analysing Incidents, Feedback and Claims to Learn from Experience Policy by April 2016. This should contain a copy of the IG incident flowchart and be made available to all staff.
    d. Changes such as the amber identifier should be communicated to all staff members as soon as practicable.

Rochdale Borough Council

14 January 2016 (follow-up to Undertaking issued 6 July 2015)

DPA – 7th Principle

Social care papers belonging to Rochdale Borough Council (RBC) were stolen from the boot of a social worker's car and subsequently discovered in a public place. These papers contained information regarding 86 individuals, with 29 of these cases including sensitive information.

At the time of this incident there was no formal data protection training provided by RBC for temporary members of staff.

Undertakings signed in July 2015:

1. All staff who become employed within the Council must receive prompt data protection training, with the completion of such training being closely monitored.
2. Refresher data protection training should be provided to staff every two years according to the Council's policy.
3. Agency, temporary and other non-permanent staff should also receive ongoing data protection training, including the monitoring of take-up.
4. All appropriate measures should be implemented as are appropriate to protect personal data against unauthorised and unlawful processing, accidental loss, destruction and/or damage.

Findings of the ICO on 14 January 2016 in relation to undertakings signed:

1. All new staff starting within the Council must now complete data protection training within fifteen working days. Failure to complete this training in the above timeframe will result in the network access of those staff being disabled. Line managers will also be able to produce reports regarding the completion status of their staff, and they must forward these to the Corporate Directors every 4-6 weeks.
2. Staff are now required to complete refresher training every two years after their previous Information Governance (IG) training session.
3. Data protection training is now mandatory for all new staff joining the Council, including all agency staff. Reports generated make no distinction between RBC staff and agency employees.
4. Further guidance has been provided to staff over the Council's intranet during April 2015, as well as e-mail, to raise awareness of how to keep personal data secure.
5. The RBC has taken appropriate steps to put plans in place to address the undertaking requirements, although the first undertaking requires further action:
   a. The RBC must take into account the nature of each new employee's role within the Council. A shorter deadline may be required for those who require regular access to a high level of personal data.
   b. Reports and statistics must differentiate between the completion status of classroom-based learning and e-learning modules.
   c. All staff must not complete any data protection training in practice.

Take our GDPR R.A.T (Readiness Assessment Tool)

How can we help?

The R.A.T is a gap analysis, maturity assessment and benchmarking tool that helps organisations to understand their current state of compliance and the nature and extent of the work they need to undertake to achieve their desired privacy end state.

The R.A.T consists of 70 questions which will be worked through during a 2 hour session with one of our privacy experts.

The results of the R.A.T will be used by PwC to generate a report on your present level of compliance with the GDPR and recommendations for compliance activities.

The General Data Protection Regulation ("GDPR") is a landmark piece of European legislation which will come into force in a year's time. It will impact every entity that holds or uses European personal data both inside and outside of Europe.

The GDPR gives rise to increased compliance requirements backed by heavy financial penalties. It introduces "Privacy by Design", "Accountability", "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 an 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 structure 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 in organisations. So, at the heart of any compliance programme is a proper understanding of what "good" looks like.

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

Individuals with good knowledge of an organisation's business processes and how personal data is used should attend. For example: data protection officers; heads of business areas and functions or other senior team members with a good understanding of the operational use of personal data; compliance personnel; legal; HR; risk; digital marketing; IT; and information security.

To take advantage of the R.A.T please contact any member of our core team.

King's College London

January 2016 (follow-up to Undertaking issued in July 2015)

DPA – 7th Principle

This London University sent a spreadsheet containing personal data in error to 22 students. This spreadsheet contained information such as exam results and other personal information belonging to 1831 students.

The data controller reported a lack of sufficient organisational measures to protect personal data, along with a lack of written supporting procedures for staff at the University. Mandatory data protection training for staff was only available on demand, resulting in 7.7% of staff receiving appropriate training.

Undertakings signed in July 2015:

1. The data controller will introduce mandatory data protection training for all staff by 31 October 2015. New employees should receive this on induction, and this should be refreshed at least every two years.
2. The data controller shall ensure that all staff who handle personal data will receive such training by 31 December 2015.
3. The completion of data protection training is fully monitored, with completion statistics reported to relevant senior management and/or working groups. Appropriate follow-up procedures should also be implemented for cases of non-compliance.
4. The data controller shall review its policies to ensure the existence of appropriate checking procedures when correspondence is sent to students. There will be written procedures to assist these by 30 September 2015.
5. Implement such other security measures as appropriate to ensure personal data is protected.

Findings of the ICO in January 2016 in relation to undertakings signed:

1. King's College London had introduced both classroom-based learning, as well as e-learning modules. Non-attendance to classroom-based training by new staff will result them having to complete an e-learning module instead. Refresher training for current staff was also planned to begin in the 2017/2018 academic year.
2. A 'Completion rates' spreadsheet indicated that 83% of all staff had engaged with the e-learning modules.
3. A Data Protection Policy was updated and approved by the Data Governance and Strategy Group in October 2015. It states how the Information Management and Compliance Team are responsible for monitoring and reporting compliance issues regarding data protection training. It also explains how new staff must complete data protection training and all other staff must complete refresher training every two years. Non-compliance may result in disciplinary action.
4. The University sent an e-mail to all staff on 29 September 2015 containing guidance on sending correspondence to students. This e-mail contained various links to guidance documents which also informs staff of the appropriate training they must complete.
5. The Information Security Policy was updated on 1 November 2015, and minutes from the IT management security meeting on 27 November 2015 indicate ongoing discussion on how to improve IT security measures.

Community Transport (Brighton, Hove & Area) Ltd

29 January 2016 (follow-up to Undertaking issued 22 July 2015)

DPA – 5th and 7th Principles

Community Transport Ltd offers various services within the Brighton and Hove area, from group and accessible passenger transport to accepting donations of second-hand furniture in order to reduce the impact on landfill sites.

A removable hard drive containing a large amount of personal data was removed by a member of staff who subsequently failed to return it. The hard drive contained a copy of the company's customer database, with records of 4,138 individual. The standard procedure at that time was for a member of staff to take a back-up drive off-site.

Undertakings signed in July 2015:

1. Portable devices containing personal data must contain encryption software in order to maximise data security.
2. Policies relevant to the storage and use of personal data are improved.
3. Policies and procedures relevant to the retention of personal data are implemented.
4. Staff are made aware of the various policies and procedures implemented and are appropriately trained how to follow that policy.
5. Staff responsible for the handling of personal data are given appropriate training upon induction and subsequent refresher training.
6. The data controller shall implement such other security measures as appropriate to ensure personal data is protected.

Findings of the ICO on 29 January 2016 in relation to undertakings signed:

1. The implementation of data encryption software had not yet been completed, pending a database upgrade.
2. Revised guidelines had been created in order to assist staff.
3. A retention policy had been created stating that customer's records will be retained for two years since the last time they used a service.
4. Staff were aware of storage policy introduced by the data controller and had received appropriate training on how to follow it.
5. Staff responsible for handling personal data were provided specific training upon induction as well as refresher training every two years.
6. Back-up disks were still being removed off-site by members of staff on a nightly basis.
7. Action had been taken by Community Transport Ltd, but further action was required to fully meet the undertakings:
    a. The implementation of encryption software, or the transfer of data to cloud-based storage should be addressed as soon as possible.
    b. Mechanisms should be created in order to monitor the compliance of training requirements.

Western Health and Social Care Trust

22 February 2016 (follow-up to Undertaking issued on 28 April 2015)

DPA – 7th Principle

The Western Health and Social Care Trust (WHSCT) provides various health and social care services to patients residing within five Council areas in Northern Ireland.

Two separate incidents resulted in this formal investigation into the Trust's compliance with the DPA. Firstly, two Trust Personal Computers were stolen as a result of a break-in to Trust premises in October 2013. One computer contained highly sensitive personal data regarding the provision of specialist mental health services. It had been deleted from the hard drive but still posed the risk of being retrieved.

The second incident occurred in June 2014, where two other patients' medical notes were disclosed to an individual who submitted a subject access request (SAR). There appeared to be no requirement for the parties involved within the SAR process to check requested notes for third party patient data.

Undertakings signed in April 2015:

1. The data controller shall maintain and regularly assess their systems for folder re-directions to maintain the security of personal data.
2. The current assent control processes shall be reviewed in order to ensure that all equipment redistributed to new staff is appropriately cleared of all personal data.
3. Physical security measures are adequate to prevent unauthorised access.
4. Policies surround SAR's regarding checks for unrelated third-party information are adequate to prevent unauthorised access to personal data. This should include specific training being provided for staff who check and redact information.
5. Regular mandatory refresher training should be provided to all staff who routinely process personal data, with training on how to follow the data controller's policies.
6. Implement such other security measures as appropriate to ensure personal data is protected.

Findings of the ICO in February 2016 in relation to undertakings signed:

1. The Trust's ICT Disposal Policy had been reviewed with an amended policy now elaborating on the redistribution of ICT equipment. The updated policy was due to be approved in March 2016.
2. PC's and laptops scheduled for disposal have their hard disks removed, and shredded by waste management companies who then provide a certification of destruction.
3. The Trust will develop a bespoke training package for SAR requests to include guidance on checking, identification, redaction and a process to follow for misfiling and the removal of third party data.
4. The WHSCT has taken appropriate steps and put plans in place to address the requirements of the undertaking, however further action is required:
    a. Current records indicated a data protection training completion rate of 16.5% for Quarters 1-3 of the current year. The Trust should aim to have all members of staff who handle personal data to receive this training as soon as possible.

British Red Cross

26 February 2016

PECR – Regulation 21

The British Red Cross (BRC) is the United Kingdom branch of the international humanitarian aid charity, The International Red Cross and Red Crescent Movement. Following an article posted within the Daily Mail on 7 July 2015, the ICO launched an investigation into the marketing practices of the BRC.

The BRC confirmed that they do not sell personal data to third party organisations, and in May 2015, decided not to share individuals' data with other charities.

The British Red Cross shall, as from the date of this Undertaking and for so long as similar standards are required by the Regulations or other successor legislation, ensure that it complies with Regulation 21 and, in particular:

1. Implement an 'opt-in' consent model for live telephone marketing calls no later than 12 months from the date of this Undertaking. Consent must be given by a clear affirmative action indicating the individual's agreement to the sharing of their data in this manner.
2. Ensure that any consented data referred to in paragraph (1) will be subject to a 24 month expiration period. After this period expires, the BRC may only make live telephone marketing calls upon receiving fresh consent from the individual.

General Dental Council

29 February 2016 (follow-up to Undertaking issues 7 September 2015)

DPA – 7th Principle

The General Dental Council (GDC) regulates all dentists working within the United Kingdom, by maintaining an updated register of all qualified and practicing dentists. The ICO was contacted by a registrant who had been sent fitness to practice allegations along with a CD containing details of these allegations in error. The intended recipient had a similar name to the registrant who received the allegations.

The controller's casework guidance and checking process around selecting the correct recipient was not followed, and the CD sent to the incorrect registrant had not been encrypted. It was established that there was an absence of corporate data protection refresher training. The data controller enforced induction data protection training, but this was not provided to existing staff. 'Masterclasses' were delivered to individual teams who processed a high amount of the most sensitive personal data, but only on an ad-hoc basis.

A further incident included the loss of a patient's set of medical records, as they had been securely destroyed in error. Upon investigation, it was evident that one employee involved in this incident had not received induction data protection training.

Undertakings signed in September 2015:

1. All current employees receive data protection training by 30 September 2015.
2. The data controller create a mandatory refresher training programme by 30 November 2015 to ensure all staff receive adequate training at least every two years.
3. The completion of data protection training should be fully monitored, with completion statistics forward to relevant senior management and/or working groups.
4. Implement such other security measures as appropriate to ensure personal data is protected.
5. In addition to the above Undertakings, the GDC will also proactively take the following steps:
    a. In relation to point (2) the data controller will extend the training programme to include the Fitness to Practise panellists and Investigating Committee members as well as the data controller's employees.
    b. The data controller shall develop a programme of more targeted training of key groups, including Fitness to Practice and Registration staff by 30 November 2015.

Findings of the ICO on 29 February 2016 in relation to undertakings signed:

1. An initial online learning module has been implemented since August 2015, with a compliance rate of 88% (due to staff turnover or staff on long term leave).
2. The GDC have worked with external training providers to create classroom-based training which has been completed by 89% of current staff.
3. Fitness to Practice and Investigating Committee members have received data protection training from the GDC.
4. Data protection training completion is monitored by the GDC, with reminder e-mails being sent to management of those staff members who did not attend training. Training completion reports are also sent to members of the Executive Management Team.
5. Further action to be taken by the GDC during 2016:
    a. All staff will be required to complete data protection refresher training through the online training module, achieving at least an 80% pass mark by 15 April 2016.
    b. A project to review the content and delivery of the corporate induction of new staff will commence in February 2016.
    c. A longer version of the data protection course has been designed for specific groups such as Fitness to Practise panellists, Registration staff and Investigating Committee members. This is due to be delivered in March 2016.
    d. Following the delivery of this extended training course, a wider review will be launched concerning the training requirements of the Fitness to Practise panellists, Registration staff and Investigation Committee members.
    e. The GDC will also explore the feasibility of providing new employees, who have not received data protection training, write-access to the Microsoft Dynamics CRM system until adequate training is received.
6. The GDC has taken appropriate steps to put plans in place to address the undertaking requirements, although further action must be taken:
    a. Data protection training needs of all staff should be clearly documented in a relevant policy of which staff are aware.

Chief Constable Wiltshire Constabulary

10 March 2016

DPA – 7th Principle

A handover file containing officer and witness statements relating to an incident involving imitation firearms and drugs, had been lost. The file was placed in the internal post, but arrived at the incorrect destination. Most of the documents were recorded electronically and could therefore be retrieved, although certain witness statements were record on paper. This resulted in some witnesses having to provide statements on a second occasion.

The data controller had no record of whether the staff member involved in this incident had received data protection training. It was further discovered that data protection training at induction was only provided for staff employed within the last ten years. No data protection training records were maintained by the data controller in respect of staff employed before this date, and there was no provision in place for refresher training, with only 30% of staff completing such training.

The data controller shall, as from the date of this Undertaking and for so long as similar standards are required by the Act or other successor legislation, ensure that personal data are processed in accordance with the Seventh Data Protection Principle in Part I of Schedule 1 to the Act, and in particular that:

1. A suitable method of delivering data protection training to all staff who handle personal and/or sensitive personal data be introduced and the attendance of such training be recorded and monitored.
2. Data protection training provided to staff be refreshed at regular intervals.
3. Appropriate records management training be delivered to all staff who regularly handle process files containing personal and/or sensitive personal data.
4. The completion of such mandatory records management training to be monitored and the results reported into a central location. This will ensure appropriate oversight of records management training uptake.
5. Implement such other security measures as appropriate to ensure personal data is protected.

Cambridgeshire Community Services NHS Trust

17 March 2016 (follow-up to Undertaking issued 20 July 2015)

DPA – 7th Principle

This NHS Trust provides services ranging from adult and child specialist health care to sexual health services to the Cambridgeshire area. The data controller reported several losses and theft of personal data. It was later discovered that the controller was only requiring their employees to complete refresher Information Governance (IG) training every two years. This was in contradiction of requirement 12-112 of the IG Toolkit which stipulates that employees who are responsible for the delivery of care must complete annual refresher training.

The data controller subsequently amended their policy in order to become compliant with requirement 12-122, although the controller has been unable to meet their target of full compliance by March 2015.

Undertakings signed in July 2015:

1. The data controller shall ensure 95% of staff are compliant with their IG training requirements by 31 August 2015.
2. Perform a review of the current training provision in order to ensure full compliance with IG Toolkit by the 30 September 2015.
3. Review procedures for following up mandatory training completion by 30 September 2015, to ensure effective action is taken in cases of non-compliance with training requirements.
4. Implement such other security measures as appropriate to ensure personal data is protected.

Findings of the ICO on 17 March 2016 in relation to undertakings signed:

1. As of September 2015, the Trust has achieved 95% compliance with IG training.
2. The Trust has introduced an Electronic Staff Record (ESR) system in order to monitor IG e-learning compliance.
3. E-mail reminders are sent to staff over the ESR system to inform them of training deadlines. Reminders are also sent to managers where staff have been non-compliant with their training requirements.
4. Where staff have completed IG-based training outside of the ESR system. They can contact the ESR helpdesk in order to register their training.
5. IG training must be completed within the first three months of employment within the Trust, thereafter refreshed on an annual basis.
6. An IG Training Programme document sets out staff responsibilities in relation to IG training. This also includes a training needs analysis for all staff groups. This document will be reviewed on an annual basis.
7. Staff also receive reminders to complete IG training through Trust-wide screensavers and a weekly newsletter.
8. In general, the Trust has taken appropriate steps and put plans in place to address the undertaking requirements and mitigate any highlighted risk.

The South Eastern Health and Social Care Trust

22 March 2016

DPA – 7th Principle

The Social Eastern Health and Social Care Trust (SEHSCT) provides a variety of health and social care services to patients in the South-East counties in Northern Ireland.

The ICO was informed of two separate incidents that occurred within the SEHSCT, with the first incident involving a locum doctor who left unsecured patients' records in a private rental property they had vacated. It became apparent that the Doctor had removed these records from Trust premises without prior senior approval.

The second incident involved an employee sending a confidential document containing highly sensitive data to her personal e-mail address, who later discovered she had entered the address incorrectly. There appeared to be a considerable lack of training provided to employees, and significant room for improvement in terms of record keeping.

The data controller shall, as from the date of this Undertaking and for so long as similar standards are required by the Act or other successor legislation, ensure that personal data are processed in accordance with the Seventh Data Protection Principle in Part I of Schedule 1 to the Act, and in particular that:

1. All staff including locum doctors, third party contractors, temporary staff as well as volunteer staff who routinely process highly sensitive data must undertake mandatory data protection and data handling induction training, and regular refresher training thereafter.
2. Provision of such training will be monitored and recorded with oversight provided at a senior level. Follow-up procedures will also be implemented by the data controller to highlight areas of non-compliance.
3. All staff including locum doctors, third party contractors, temporary staff as well as volunteer staff who routinely process highly sensitive data will be made aware of the content and location of the controller's policies relating to personal data. A mechanism, if not already created, should be implemented to update staff of any changes made to these policies.
4. Implement such other security measures as appropriate to ensure personal data is protected.

Anxiety UK

22 March 2016 (follow-up to Undertaking issued 3 August 2015)

DPA – 7th Principle

This charity works to support individuals who suffer from anxiety, or anxiety-based depression. In February 2015, the ICO received reports that personal and sensitive personal data held within a password-protected section of Anxiety UK's website was made available via an internet search engine. The data controller had failed to ensure that the data processor had sufficient technical measures in place to properly secure its systems. Out of date membership details were also located on this website, indicating a lack of quality assurance controls.

Undertakings signed in August 2015:

1. Periodic security testing of the website shall be implemented, with the scope of the testing based on the risks posed to personal data processed on the website.
2. Adequate contractual controls and supporting review mechanisms will be implemented to ensure data processors comply with the 7th Principle of the DPA.
3. Appropriate retention, review and disposal controls will be implemented to ensure that data is not held longer than is necessary, in compliance with the 5th Principle of the DPA.
4. Implement such other security measures as appropriate to ensure personal data is protected.

Findings of the ICO on 22 March 2016 in relation to undertakings signed:

1. Anxiety UK has commissioned a new website designed to reduce exposure to vulnerabilities. The new website was fully penetration tested before it went live and annual penetration tests will be conducted on it as well as quarterly scans by a website security company.
2. Appropriate retention, review and disposal controls have been implemented. This includes the creation of a Data Retention Policy and measures to securely dispose of redundant IT equipment.
3. Further actions have been taken:
    a. An external data security review was performed in January 2016.
    b. Information security policies have been updated.
    c. The Anxiety UK Board of Trustees is monitoring an Information Governance Project plan.
    d. Staff data protection training has been implemented which is tested by a quiz.
4. Appropriate steps have been taken to put plans in place to address the requirements of the undertaking, however further work needs to be completed:
    a. An external data security review was undertaken by an external security consultant in January 2016. Anxiety UK should enter into data sharing agreements with all partners in the supply chain.

Age International

24 March 2016

PECR – Regulation 21

Age International is a charity devoted to helping older people in developing countries. After an article published on 7 July 2015 by the Daily Mail, the ICO launched an investigation into the direct marketing practices of the charity sector.

Age International confirmed (amongst other things) that it does not sell personal data to third party organisations.

Age International shall, as from the date of this Undertaking and for so long as similar standards are required by the Regulations or other successor legislation, ensure that it complies with Regulation 21 and, in particular:

1. Implement an 'opt-in' consent model for live telephone marketing calls no later than 12 months from the date of this Undertaking. Consent must be given by a clear affirmative action on behalf of the individual.
2. Ensure that any consented data referred to in point (1) will be subjected to a 24 month expiration period. Once this time period expires, Age International will only make further live telephone marketing calls if fresh consent is received from the individual.

Flybe Limited

1 April 2016 (follow-up to Undertaking issued 16 February 2015)

DPA – 7th Principle

Flybe Ltd is a commercial passenger airline based in Exeter within the United Kingdom. A temporary employee e-mailed a scanned picture of an individual's passport to his personal e-mail account. This particular employee worked within the 'air side pass' section, responsible processing and providing 'airside' passes for employees.

It was later discovered that, at the time of the incident, Flybe did not provide data protection training to all staff who process personal data, including the member of staff involved in this incident. This investigation also revealed an inadequate Data Protection Policy within Flybe which provided very little advice.

It was also revealed that the temporary employee in this case accessed various forms of sensitive data as part of the process to issue 'airside' passes to permanent staff. The ICO was concerned that such access had been granted without due consideration to carrying out similar background checks to those afforded to permanent employees.

Undertakings signed in February 2015:

1. The policy covering the storage and use of personal data is revised in light of this incident, to include detail on how such data will be protected.
2. Staff are aware of the data controller's policy for the storage and use of personal data and are appropriately trained on how to follow it.
3. Permanent and temporary staff responsible for the handling of personal data are given appropriate, specific training upon induction. Refresher training should also be provided annually, with completion rates monitored and recorded.
4. Ensure the reliability of any temporary employees who have access to personal data and where appropriate, bring these in line with the checks undertaken when employing permanent staff.
5. Implement such other security measures as appropriate to ensure personal data is protected.

Findings of the ICO on 1 April 2016 in relation to undertakings signed:

1. Revised the information security and handling policy.
2. Produced a quick reference guide for staff on the information security and handling policy, which is provided to staff on induction.
3. An information security video is shown to all members of staff at induction.
4. Implemented e-learning training with a pass mark of 80%.
5. Training completion statistics are reported to the Executive Committee, along with statistics of how many staff have read and understood the information security and handling policy.

6. All 'high risk' roles now have specific data protection training provided by an external DPA specialist.
7. Staff that access highly confidential and sensitive personal data are given training prior to being given access to personal data.
8. Staff who require access to highly confidential personal data require enhanced background checks.
9. The information asset register has been developed which assists with system access controls.
10. The whistle blowing policy has been relaunched to encourage employees to report security incidents confidentially.
11. Flybe Limited have become members of the ISF and the ISF have carried out an information security health check.
12. The Audit Committee are regularly updated on plans to improve Flybe Limited's information and cyber security resilience.
13. A weekly report is sent to the Executive Committee with information concerning various security matters, and their detection and prevention. This report includes among others, information about systems review, supplier audit, crisis management, and awareness campaigns.
14. Flybe Limited have taken appropriate steps to and put plans in place to address the undertaking requirements, but should take further steps:
    a. Ensure all employees complete information security training and read the relevant policies before accessing personal data.
    b. Display their new data protection awareness posters, as planned.
    c. To roll out the new DPA e-learning module, as planned.

Brunel University London

7 April 2016 (follow-up to Undertaking issued 28 July 2015)

DPA – 7th Principle

This University located in Uxbridge, London lost ten boxes containing 7 personnel files and 61 TUPE transfer files. This occurred following an office renovation to remove asbestos. These boxes were among others locked in a room during the renovation, but on return to the office staff members realised that some of the boxes were missing. Brunel University did have a number of policies and procedures in place at the time of the breach, but only had a staff completion rate for data protection training of less than 10%.

Undertakings signed in July 2015:

1. Ensure that staff who routinely process personal data shall receive training in the requirements of the DPA upon induction.
2. Regular mandatory refresher training in data protection shall be provided to all staff members whose role involves the routine processing of personal data. Uptake of this training shall be monitored to ensure all staff members receive regular refresher training annually.
3. Implement such other security measures as appropriate to ensure personal data is protected.

Findings of the ICO on 7 April 2016 in relation to undertakings signed:

1. The completion of data protection training is now mandatory for all non-academic staff in order to complete probation at 6 and 12 months.
2. Data protection training is now available via an e-learning module in the University's intranet.
3. Senior staff have received a briefing from the Information Access Officer on the DPA and the importance of compliance when processing personal data.
4. Face-to-face briefings and refresher sessions on data protection have been scheduled for staff over the next 6 months.
5. There is now a set of criteria implemented to guide staff on when to undertake data protection training and in which format.
6. A data classification scheme for information held and generated by the University has been drafted and should be implemented before the end of 2016.
7. The University is in the process of reviewing its overall approach to cyber and information security. This includes the development of an updated training and awareness programme.
8. Brunel University has taken appropriate steps and put plans in place to address the undertaking requirements, but should take further action:
    a. Ensure the data protection training programme is rolled out to appropriate academic staff as soon as is feasible.
    b. Ensure that completion of refresher training once a staff member has passed probation is robustly monitored.

Croydon Health Services NHS Trust

15 April 2016 (follow-up to Undertaking issued 14 December 2015)

DPA – 7th Principle

Croydon Health Services (CHS) suffered a breach in data security when a mailing responding to a compliant was sent to an incorrect address. The mailing contained the complaint response letter, copies of notes from meetings held as part of the complaint investigation process, as well as sensitive information including clinical information relating to the patient. This incident followed several others of a similar nature previously reported involving the misdirection of clinical correspondence. This particular error was made by a temporary employee who had not received appropriate training regarding the role they were expected to fulfil. There was a lack of formal checking procedures, and key recommendations from previous investigation reports had not been implemented. These factors combined with a lack of senior managerial oversight was thought to contribute to the occurrence of this breach.

A second incident occurred involving the loss of a Birth Register covering dates from April 2009 to May 2010, but was subsequently recovered.

Undertakings signed on 14 December 2015:

1. The achievement of IG training targets and staff awareness of IG issue is given key priority subject to regular ongoing review, testing and oversight by the Information Governance Committee.
2. All staff in the Complaints team complete data protection training on an annual basis, which is in addition to the mandatory information governance training.
3. The attendance at data protection training sessions is monitored and there are appropriate follow up procedures in place to ensure completion.
4. A thorough review of data flows and an information risk assessment of information assets within the Trust are completed together with a detailed and updated Information Asset Register (IAR). This is to ensure oversight of the variety of sites and records management practices operating within the Trust. The final report in relation to this to be submitted to the ICO by 31 March 2016.
5. The approved option for legacy record disposal should be implemented as soon as is practicable, with progress regularly monitored and reported at each Information Governance Committee.
6. Correspondence checking procedures throughout the organisation are captured in a clearly written procedural document which is brought to the attention of all relevant staff who are required to sign to the effect that they are aware and understand the procedure.
7. The implementation of recommendations from data protection incident investigation reports is closely monitored, and evidence of completion is made available to the relevant committees with oversight for data protection and information governance matters.
8. The data controller shall provide evidence of the implementation of the above measures by 31 March 16.
9. Implement such other security measures as appropriate to ensure personal data is protected.

Findings of the ICO on 15 April 2016 in relation to undertakings signed:

1. CHS has given key priority to achieving IG training targets and staff awareness. There is a regular review and testing of staff knowledge. However, their initial target was 95% IG training completion by March 2016, and they are currently at 93% completion.
2. All staff on the complaints team have completed data protection training in addition to the mandatory IG training. The training covers Consent, Confidentiality, Security and Records Management.
3. The ICO were informed that attendance at data protection training is monitored with appropriate follow-up procedures.
4. CHS has reviewed information assets for data flows and conducted information risk assessments. A consultancy had been commissioned to complete the IAR and data flow mapping in 2014. CHS reviewed this information, tracked and updated it while assigning individual ownership and directorates in 2016. The ICO were supplied with a report that details the work to monitor data flows being completed.
5. CHS has implemented a records disposal option for legacy records.
6. A correspondence checking procedure has been implemented and brought to the attention of all staff. Staff have signed to confirm that they are aware of this procedure and understand its requirements.
7. The implementation of the recommendations from the data protection incident investigation report is monitored.
8. The ICO were supplied with evidence in relation to progress against the objectives in the undertaking within the allotted time.
9. As well as the requirements for the undertaking, the CHS has also updated the following documents:
    a. Confidentiality and Data Protection Policy
    b. IG Framework
    c. Information Security Policy
    d. Staff Confidentiality Code of Conduct
    e. Records Management Strategy and Policy
10. The CHS has also publicised their IG pages on their intranet.
11. The CHS has taken appropriate steps and put plans in place to address some of the requirements of the undertaking, however further work needs to be completed:
    a. Ensure that the work around training continues to improve IG training figures and meet training targets.
    b. Ensure that legacy record destruction continues.

Health and Social Care Information Centre (HSCIC)

20 April 2016

DPA – 1st Principle

The HSCIC is the national provider of information, data and IT systems for health and social care. In January 2014 a leaflet was sent to all households in England offering patients the chance to opt out of their personal information being shared for purposes other than direct care. These were known as 'Type 2 objections', and patients were instructed to inform their GP if they applied these objections to their personal confidential data.

Due to legal and technological reasons, the HSCIC was not able to collect, record or implement the Type 2 objections registered by patients with their GP's, resulting in approximately 700,000 Type 2 objections not being implemented. This resulted in the HSCIC sharing patients' data with other organisations against their wishes.

The ICO was concerned about the way in which HSCIC had communicated with the general public about this matter. Apart from placing a statement on the HSCIC website, no further steps had been taken to contact those affected.

This issue of sharing patient data on a national basis is currently under the review of Dame Fiona Caldicott, the National Data Guardian. This review aims to clarify the policy framework regarding patient data and opt out policies across the Health and Care System.

Undertakings signed in April 2016:

1. HSCIC should establish and operate a system to process and uphold Type 2 objections, in accordance with the Direction from the Secretary of State within six months of the date of this undertaking.
2. Measures should be enforced to make all patients affected aware of the incident. HSCIC should also inform the patients that their personal data may have been shared with third parties against their wishes. This should be completed within six months.
3. Ensure measures are put in place so that any patients who have previously registered a Type 2 objection, or those registered in the future, are provided with clear fair processing information enabling them to understand how the objection will be applied and how their data will be used.
4. HSCIC should contact recipients of data sets it provided between January 2014 and April 2016 to make them aware of the possibility that those data sets may include records relating to patients who have chosen to opt out. This should be completed within three months.
5. HSCIC should contact recipients of data sets it provided between January 2014 and April 2016 where there was an agreement to allowing the recipient to disseminate the data, to make them aware that this data should no longer be disseminated. This should be completed within three months.
6. HSCIC should contact recipients of data sets it provided between January 2014 and April 2016 to inform them that, where possible, the data sets should be destroyed and replaced with a new data set which reflects patient opt outs. A certificate of destruction will be collected where possible for all data destroyed or deleted.
7. HSCIC should revisit the matter of objections following the completion of the National Data Guardian review, and consider whether its processes can be modified to enable Type 2 objections to be applied where this is not currently possible.

Doncaster Metropolitan Borough Council (DMBC)

24 March 2016 (follow-up to Undertaking issued 27 July 2015)

DPA – 7th Principle

DMBC's data controller lost 66 records of families requiring Health services within the Doncaster borough, resulting from an internal office move. There is no evidence to suggest these files are in the public domain and the ICO is happy that there were adequate physical security measures in place at the time of the incident.

However upon investigation by the ICO, a very low staff completion rate of data protection training was revealed. Staff were only required to undertake data protection training every three years, which is inconsistent with the ICO's guidance.

Undertakings signed in July 2015:

1. Conduct a training need analysis for all roles within the organisation to ascertain the level of data protection awareness required for the role, and the frequency of refresher training each individual should receive. This should be completed by January 2016.
2. Deliver mandatory data protection training to the relevant individuals, and at the intervals agreed within the aforementioned training need analysis.
3. Ensure all staff required to undertake mandatory training complete the training within agreed timescales.

Findings of the ICO on 24 March 2016 in relation to undertakings signed:

1. It was reported that 'the Data Protection Officer and Information Management Officer are liaising with the Organisational Development Team to identify any e-learning modules held on the Learning Pool which can help staff carry out role specific data protection training'. The Data Protection Officer (DPO) is also developing an annual refresher module for all staff to undertake. However, DMBC has not met the requirement to conduct a comprehensive training need analysis by January 2016.
2. DMBC advised that online data protection training is currently available and future training modules are being developed. Classroom based training has also been reintroduced for staff who do not have access to a computer. However, DMBC's approach is not being informed by a comprehensive training need analysis.
3. Data protection training has been made a mandatory element of staff appraisals. People Managers are required to ensure that staff are appropriately trained to 'effectively manage data and information'. They must also ensure staff keep up-to-date with e-learning training. The mandatory data protection refresher module is still being developed.
4. DMBC has not taken appropriate steps to address the requirements of the undertaking and should implement the following without undue delay:
   a. Suitable method of providing data protection training to all staff who handle personal or sensitive personal data. Attendance and completion should be recorded and monitored.
   b. Data protection training should be refreshed at regular intervals.
   c. A method for monitoring the completion of mandatory records management training, with the results being reported into a central location to ensure appropriate oversight of training uptake.
   d. If a further breach occurs, which the ICO considers could have been prevented or minimised by such training having been provided, ICO will consider formal action.

Martin & Company

20 April 2016 (follow-up to Undertaking issued 14 September 2015)

DPA – 7th Principle

Martin & Co. is a solicitors firm based in Ayr, Scotland. A DVD containing evidence to be used in a criminal trial was lost. The disk was not encrypted, and it contained limited footage of the defendant entering a room. The DVD was held in Crown Office & Procurator Fiscal Service offices in Kilmarnock, when a colleague from another firm was asked to collect the DVD on Martin & Company's behalf. The DVD was mislaid by the third party before it could be delivered to Martin & Co. Therefore the DVD was not in the possession of Martin & Co. when lost. This investigation revealed multiple shortcomings within the data protection procedures of the solicitors firm. Guidance to staff regarding data protection compliance as well as formal training was lacking. There was no standardised procedure in place for staff to follow when arranging to collect personal data outside of the office environment.

Undertakings signed in September 2015:

1. Appropriate procedures for the collection of paper and electronic media containing personal and sensitive data from third parties are implemented within three months.
2. Safeguards are implemented within three months to ensure that, where possible, portable media used to process sensitive data will be encrypted using encryption software that meets current standards or equivalent.
3. A Data Protection Policy is implemented within three months.
4. Staff are aware of the data controller's policy for the storage and use of personal data and are appropriately trained on how to adhere to that policy.
5. Staff responsible for handling personal data are given appropriate, specific training upon induction. The training should be refreshed annually.
6. Implement such other security measures as appropriate to ensure personal data is protected.

Findings of the ICO on 20 April 2016 in relation to undertakings signed:

1. Have implemented procedures relating to the collection of paper and electronic media containing sensitive and personal data from third parties, giving specific instructions in relation to Crown productions, anti-money laundering documentation and civil department records.
2. Staff have been made aware of these policies and provided with guidance on how to follow them via a staff training memo. This memo provided general data protection guidance, with a Q&A session being implemented for staff to ask further questions. This was provided in November 2015 (or on induction if after this date) and will be refreshed annually.
3. Martin & Co. have taken appropriate steps and put plans in place to address some of the requirements of the undertaking, however further work is required:
   a. It has not been possible to enforce encryption software as DVD's provided by the Crown Office are received in an unencrypted state and cannot be encrypted upon receipt. The ICO is working with the Crown Office & Procurator Fiscal Service and the Scottish Government on ways to improve information security.
   b. Martin & Co. currently has a policy enabling company e-mails to be forwarded to users' personal Hotmail accounts, which the ICO would consider to be poor practice.
   c. Staff policy documents and guidelines should be proof read to correct grammatical errors and inaccuracies.
   d. Data protection training is currently in the form of a memo. Martin & Co. may wish to consider introducing more comprehensive training such as the free e-learning module provided by the National Archives.

Sirona Care and Health

10 May 2016 (follow-up to Undertaking issued 13 November 2015)

DPA – 7th Principle

Sirona Care & Health ("Sirona") provide a range of health and wellbeing services from clinics and treatments, to providing information on learning disabilities and mental health. In March 2015, an email containing sensitive personal data was sent to a previous service user in error by a Sirona employee. This email contained sensitive details relating to three service users including names, dates of birth, NHS numbers, addresses and medical details.

Sirona only 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 any detailed guidance for checking email addresses or deleting those no longer in use. The ICO found that the Sirona employee in question had not received information governance training for over two years and only 66% of staff were up-to-date with this training. In addition, the ICO held that Sirona may not have taken sufficient steps to act on previous advice regarding a previous incident where Sirona was unable to demonstrate staff compliance with information governance training.

Undertakings signed in November 2015:

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

Findings of the ICO on 10 May 2016 in relation to undertakings signed:

1. Annual classroom-based refresher training will be implemented in June 2016 in order to improve compliance for staff members. This training will cover both data protection and information governance.
2. The Learning and Development department will be maintaining a log of staff compliance with both mandatory and refresher training that staff attend. It will also have the responsibility of chasing staff member's compliance.
3. Policies regarding email checking procedures have been reviewed by an IG consultant, resulting in an updated Safe Haven Policy. This policy has five sections detailing the procedures staff need to follow when sending an email.
4. More security measures have been implemented to flag all emails sent by staff containing personal data. If any are sent insecurely, the IG Consultant and IT Operations Manager will be automatically notified. A specialist IT company has also been contacted to look into current firewalls, malware and virus protection. Further protective software has been purchased and installed to better identify potential risks.
5. Sirona has taken appropriate steps and put plans in place to address the requirements of the undertaking and to mitigate the risks highlighted.

Leeds Community Healthcare NHS Trust

26 May 2016 (follow-up to Undertaking issued 13 November 2015)

DPA - 7th Principle

Two letters containing sensitive personal data relating to a patient had been included in the response to another person's subject access request. The letters in question were filed incorrectly, and several opportunities to identify the wrongly filed letters were then missed before the information was sent.

Further investigation revealed that temporary staff within Leeds Community Healthcare NHS Trust (the "Trust") may not have received data protection training unless employed for over three months. The Trust's policies also set out that Information Governance training, which includes data protection, is only refreshed every three years.

Undertakings signed in November 2015:

1. Ensure that all staff processing personal data, whether permanent or otherwise, are provided with sufficient 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 is refreshed annually.
6. Implement such other security measures as appropriate to ensure personal data is protected.

Findings of the ICO on 19 May 2016 in relation to undertakings signed:

1. All staff, students and agency workers are now required to complete the HSCIC training. The Trust has reported that the Electronic Staff Record has been updated to reflect that the training is mandatory.
2. Information has been provided to staff regarding the requirement to complete Information Governance ("IG") training every 12 months. Staff required to attend training were sent reminder emails informing them to complete such training by March 2016.
3. The induction training checklist has been updated to ensure that new starters complete IG training on their first day of employment.
4. Standard operating procedures regarding IG training compliance have been produced. These involve restricting new starters' access to clinical systems where IG training has not been completed and revoking access to clinical systems for existing staff where annual refresher training has not been completed.
5. Training records for IG training compliance are maintained by the Trust, which indicates whether an employee's training is up to date, expiring shortly or has expired.
6. Notifications are sent to staff line managers informing them of staff who are due to complete refresher training in the upcoming months.
7. The Trust has carried out a workshop for staff responsible for handling subject access requests.
8. The Trust has taken appropriate steps and put plans in place to address some of the requirements of the undertaking, however further work is required which includes:
    a. Reviewing and updating subject access request policies and procedures.
    b. Providing specific role-based training to staff involved with subject access requests annually.
    c. Reviewing and updating IG policies and procedures.
    d. Providing specific role-based data protection training for all staff involved in handling personal data.

Wolverhampton City Council

6 June 2016

DPA – 7th Principle

In November 2015, Wolverhampton City Council (the "Council") requested a report to be produced by its payroll department. Personal information of 9,858 employees at 73 educational establishments was subsequently sent in error to an external recipient via email. The ICO's investigation revealed that although data protection training was mandatory at induction and refreshed at regular intervals when this incident occurred, the Council did not have a reliable method of monitoring the completion of refresher training.

The ICO had conducted an audit of the Council in 2011 and highlighted that refresher training should be given at regular intervals. A follow-up conducted in August 2012, provided the Council with recommendations to maintain logs of staff attendance at training. Further, in 2014, the ICO served an Enforcement Notice on the Council which required it to "ensure that all staff have completed the 'Protecting Information' e-learning module. Although the ICO was satisfied that the terms of the Enforcement Notice was met, the ICO remained concerned at the Council's failure to establish an effective mechanism to monitor and implement refresher training.

Undertakings signed in June 2016:

1. Devise and implement a system to ensure that completion of data protection training is monitored and procedures are in place to ensure that staff who have not completed training within the specified time period do so promptly. This should be completed within three months.
2. Ensure that all staff handling personal data receive data protection training and this training is refreshed at regular intervals, not exceeding two years.
3. Ensure that (i) staff handling sensitive personal data receive refresher training within six months of the date of this undertaking; and (ii) all other staff have received refresher training within nine months of the date of this undertaking.

Although the Council has largely taken appropriate steps to comply with the undertaking, the ICO advise that they continue work in the following areas to further improve their data protection compliance:

1. WCC should ensure that they monitor and produce statistical reporting information for the protecting information learning module, specifically in respect of employees that handle sensitive personal information.
2. As line managers are responsible for ensuring that their team/s completes any mandatory training, WCC should continue to look at providing managers with an additional dashboard solution that will provide them with information about which staff have completed the protecting information e-learning training.
3. WCC should consider producing a training communications plan each year to ensure continuous awareness of the protecting information e-learning training and the requirements of the Data Protection Act.

Northern Health & Social Care Trust

19 July 2016

DPA – 7th principle

The ICO was notified by Northern Health & Social Care Trust (the "Trust") that 11 emails intended for a doctor's personal non-trust email account were sent to a member of the public with the same name over a two year period. Although not all of the emails contained personal data, on one occasion, an email contained sensitive personal data relating to a patient. The ICO's investigations later revealed that none of the emails were securely protected in accordance with the Trust's email policy. Further, and although the recipient advised the senders of the emails they had been incorrectly sent to the wrong address, this was not escalated as an information governance incident. The Trust only became aware of the incident when the recipient's wife contacted the information governance team directly.

The ICO had investigated previous incidents at the Trust which uncovered that the take up of staff training was low and that staff were unaware of the policy and procedure for reporting information governance incidents.

The data controller shall, as from the date of this Undertaking and for so long as similar standards are required by the Act or other successor legislation, ensure that personal data are processed in accordance with the seventh Data Protection Principle in Part I of Schedule 1 to the Act, and in particular that:

1. Ensure that all staff whose role involves the routine processing of personal and sensitive personal data undertake mandatory data protection and data handling induction training and regular refresher training.
2. Ensure that provision of such training is recorded and monitored with oversight provided at a senior level against agreed Key Performance Indicators to ensure completion. In addition, follow-up procedures must also be implemented to ensure that staff who have not attended/completed training do so as soon as practicable.
3. Ensure that all staff are aware of the content and location of the Trust's policies and procedures relating to the processing of personal data, specifically the procedure for reporting and recording information governance breaches. A mechanism to ensure that staff are updated of any changes to these policies and procedures should also be implemented (if not already in place).
4. Implement such other security measures as appropriate to ensure that personal data is protected against unauthorised and unlawful processing, accidental loss, destruction, and or damage.

Kent Police

8 August 2016

DPA – 1st Principle

In March 2014, Kent Police erroneously disclosed a CD containing entire contents of an individual's mobile phone. The individual in question had accused her partner of domestic abuse and the contents of the phone had been disclosed to her partner's solicitor. The individual volunteered her phone to Kent Police as evidence given that it contained a video recording which supported her allegation. Kent Police stated that it was necessary to (i) download the entire contents of the phone for technical reasons due to the complexity of the device; and (ii) retain this data as unused material in order to comply with the Criminal Procedure and Investigations Act 1996.

Investigations revealed that the individual was not informed by Kent Police of the need to download and retain the entire contents of the phone. There was also no fair processing notice to explain to the individual what she would be consenting to by providing her phone to Kent Police. The ICO therefore considered that the personal data was not processed fairly, as informed consent was not obtained.

Following the reporting of this incident, a report was published by the Association of Chief Police Officers regarding forensic mobile device examination. This report notes that police do have powers to seize and examine mobile devices where the device owner refuses to give consent. However, it makes recommendations that police should first obtain explicit, informed consent from individuals when extracting data from their mobile devices. Kent Police did not take steps to address these recommendations despite the ICO bringing this report to its attention several times throughout the course of the investigation.

The data controller shall, as from the date of this Undertaking and for so long as similar standards are required by the Act or other successor legislation, ensure that personal data are processed in accordance with the First Data Protection Principle in Part I of Schedule 1 to the Act, and in particular that:

1. Develop written procedures and other supporting documentation for their relevant staff (e.g. scripts for officers to use, training manuals) around the extraction of data from mobile devices which emphasise that explicit, informed consent should be sought from victims and witnesses of crime in the first instance.
2. Create a fair processing notice for victims and witnesses of crime to read and sign, which clearly explains which personal data will be extracted from their mobile device and how this will be processed.

3. Where technically possible, limit the extraction of data from the mobile devices from victims and witnesses of crime to relevant data sets. Where technical requirements result in the total extraction of binary data, only relevant data sets will be converted into readable format and processed as required by the Criminal Procedure and Investigations Act 1996. Any irrelevant information in a readable format identified as such by the Disclosure Officer shall be deleted.
4. Ensure that developments and guidance around the extraction of data from mobile devices are tracked and promptly take action to address any recommendations relating to compliance with the Data Protection Act 1998 arising from this.
5. Implement such other security measures as appropriate to ensure that personal data is protected against unauthorised and unlawful processing, accidental loss, destruction and/or damage.

Falkirk Council

12 September 2016

DPA – 7th principle

On 12 March 2015, Falkirk Council (the "Council") informed the ICO of a data breach which occurred following a subject access request made by an individual to the Council. The individual received the expected documents from the Council with additional documents relating to an unrelated third party. Some of the data disclosed related to information as to the physical or mental health condition of certain data subjects.

This error occurred due to incorrect filing of documents and it was apparent that the documents were not checked to ensure that only relevant documents were passed to the individual who made the request. During investigations, it was also revealed that only 11.4% of Council employees had completed one or more sections of their data protection training modules.

Undertakings signed in August 2016:

1. Provide training to all staff members who handle personal data as part of their job role within nine months. This training will be mandatory and will be refreshed annually.
2. Implement a process for monitoring (and following up) attendance at such training, or completion of online training within six months. Corporate training KPIs will be reported to and over seen by a relevant senior management group or board.
3. Issue improved guidance to staff members who routinely handle subject access requests within six months.
4. Produce a high level data protection policy, setting out commitments to the protection of personal data and the general standards the Council will adhere to. This is to be communicated to all relevant staff members within one month of completion and should be referenced in the mandatory training.

Findings of the ICO on 9 September 2016 in relation to undertakings signed:

The ICO's follow-up assessment demonstrated that the Council has taken appropriate steps by:

1. Implementing a data protection and information security e-learning module, which is mandatory for all 6,800 employees (from a total workforce of 7,771) who handle personal data. As of 31 July 2016, 76% of the 6,800 employees have completed the e-learning or attended a presentation. The Council has also committed to an annual refresher requirement in respect of data protection training.
2. Issuing monthly e-learning completion reports to Service Directors. The Corporate Management Team ("CMT") have ratified key performance indicators in respect of the percentages of employees who handle personal data that have completed the e-learning or alternative training. The CMT will receive a report on these KPIs on 19 September 2016 and on an annual basis going forward.
3. Adding updated subject access guidance to the intranet, which includes a subject access process flowchart, template covering letter for subject access responses and a more general redaction note.
4. Ratifying a Data Protection Policy, which outlines a commitment to comply with the Data Protection Act 1998, and subsequently communicating this Policy to all staff. However, the Council needs to complete further work to fully address the undertakings signed, namely ensuring that:
    a. the remaining 24% of the Council's 6,800 employees and all new employees who will also handle personal data, either complete the e-learning or attend the alternative presentation.
    b. the Council regularly generate completion reports in respect of the presentations for employees without network access and periodically monitor these at a corporate, as well as at Service, level.
    c. subject access guidance and/or policies which are intended for employees who routinely handle subject access requests, closely align with the specific process for handling such requests in practice at the Council; and
    d. the Data Protection Policy includes a reference to the subject access guidance and/or policies.

Cornwall Council

4 October 2016

DPA – 1st Principle

In the past two years, eight data breaches suffered by Cornwall Council (the "Council") have been reported to the ICO. Following investigations into two incidents in particular, (which involved disclosures made in error) it was revealed that some staff members had not received data protection training and that the general uptake of training was unsatisfactory. On 29 June 2015, it was agreed that the Council would supply information regarding the uptake of training to the ICO on a monthly basis.

Although the uptake had improved, it was still considered unsatisfactory. Figures supplied in August 2015 showed the total uptake of training to be 17% of the workforce and by March 2016, this figure had risen to 55%.

The data controller shall, as from the date of this Undertaking and for so long as similar standards are required by the Act or other successor legislation, ensure that personal data are processed in accordance with the Seventh Data Protection Principle in Part I of Schedule 1 to the Act, and in particular that:

1. All current staff members responsible for the handling of personal data should receive appropriate, specific data protection training. This process should be completed within three months.
2. Such training should be refreshed at regular intervals, not exceeding two years and its provision monitored and recorded.
3. New staff members responsible for the handling of personal data are given appropriate, specific data protection training upon induction.

British Showjumping

12 October 2016

DPA – 7th Principle

A file containing a large section of British Showjumping's ("BS") membership database had been 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 kept for longer than necessary and had the same name as the file usually sent to the distribution group. The ICO's investigation revealed that British Show Jumping did not have any relevant policies or procedures that provided appropriate advice provided to staff on emailing personal data or on retention and naming of documents on shared drives.

Undertakings signed in August 2015:

1. Ensure that guidance is provided to staff regarding checking the content and attachments of emails containing personal data before they are sent, and that this guidance is formalised in an appropriate policy or procedure.
2. Ensure that an appropriate policy or procedure regarding the use of shared network drives is introduced which includes advice on retention and the use of appropriate file names.
3. Implement such other security measures as are appropriate to ensure that personal data is protected against unauthorised and unlawful processing, accidental loss, destruction, and/or damage.

Findings of the ICO on 12 October 2016 in relation to the undertakings signed:

BS confirmed that it has taken the following steps (amongst others):

1. BS has seconded an Information Governance and Data Protection Director.
2. Procedures governing the transmission of personal and sensitive data have been implemented and formally documented in the form of Standards. The Standards provide detailed guidance on the secure methods to be used for transferring data and the circumstances in which approval must be sought from an appropriate member of staff prior to transfer.
3. The Standard for Data Transmission also documents the procedure for the removal of member data from BS's member system; the removal of this data is now restricted to relevant senior members of staff and for purposes authorised by BS's Chief Executive only.
4. BS has undertaken a review of all data held on network drives and has restricted access to folders containing personal data. Member information identified as inaccurate, out-of-date or no longer required has been securely disposed of by the ICT department.
5. Guidance regarding the use of shared network drives has been formally documented in the form of a Standard. The Standard includes guidance on file naming conventions and version control. Shared network drives will be reviewed on a regular basis to ensure that data is accurate, up-to-date and not held for longer than is necessary.
6. Additional security measures that have been put in place include the implementation of documented procedures governing the management of passwords and a Remote Working Policy.
7. The above policies and procedures have been issued to, and discussed with, all existing members of staff. All new starters are issued with the policies and procedures and are required to sign to confirm their understanding. Training has also been provided to all members of staff.
8. BS has reported that staff members have embraced the new procedures and that they are working well within the organisation. BS has not had any information security incidents reported to the ICO since the breach in September 2014.
9. BS also plans to host a Data Action Network event in November 2016, where BS's Chief Executive will talk about the learning outcomes following the breach to colleagues within the sports sector.

South Eastern Health and Social Care Trust

24 October 2016

DPA – 1st Principle

Two separate incidents involving the disclosure of personal data in error led the ICO to undertake a formal investigation into South Eastern Health and Social Care Trust (the "Trust"). One incident involved a locum doctor who left unsecured patients' records in a private rental property they had vacated. The other incident involved a staff member who emailed a confidential document containing extremely sensitive information to an unintended email address having incorrectly entered her own email address. Investigations of both incidents uncovered shortcomings in relation to staff training and uptake of training by staff members. The ICO found that both record keeping and the process in place to ensure that training is mandated could be improved.

Undertakings signed in March 2016:

1. Ensure that all staff, including locum doctors, whose role involves the routine processing of personal and sensitive personal data undertake mandatory data protection induction training and regular refresher training.
2. Ensure that provision of such training is recorded and monitored with oversight provided at a senior level against agreed KPIs to ensure completion. In addition, the Trust must implement follow-up procedures to ensure that staff who have not attended/completed training do so as soon as practicable.
3. Ensure that staff, including Locum Doctors, are aware of the content and location of the Trusts' policies and procedures relating to the processing of personal data. A mechanism to ensure that staff are updated of any changes to these policies and procedures should also be implemented (if not already in place).
4. Implement such other security measures as are appropriate to ensure that personal data is protected against unauthorised and unlawful processing, accidental loss, destruction, and/or damage.

Findings of the ICO on 24 October 2016 in relation to undertakings signed:

The Trust has confirmed that it has taken the following steps (amongst others):

1. Data Protection training is mandatory and always provided at the time of induction. Refresher training is given every three years. A campaign took place over summer this year to make sure all staff completed the e-learning data protection training. In addition, a comprehensive information governance training booklet has been created for all staff who do not have access to email or a PC. This booklet will also be given to locum doctors when they start at the Trust. They will need to sign a form to say they have received this.
2. All staff in the Trust are required to complete the e-learning data protection training by 1 June 2016. The Trusts EMT receive regular statistics on the compliance with the data protection training plan. EMT weekly reports are also issued to all Assistant Directors. All Managers have been asked to ensure there are plans in place to make sure all staff who are on long term sickness absence will get the IG training as soon as they return to work.
3. All the Trust's policies and procedures are made available on their 'i-connect' site. The information governance specific policies are also published on the information governance team's page of the 'i-connect' site. Staff are made aware of said policies and procedures in their corporate and local induction.
4. The Trust has gained assurance from managers stating students and contract holders have now completed data protection training. The Trust is promoting staff responsibilities with their compliance with the data protection act. The Trust is continuing to review information governance incidents and sharing any information learnt across the appropriate departments.

Royal Bank of Scotland

8 November 2016

DPA – 7th Principle

In October 2014, dozens of faxes containing personal data were sent to an incorrect fax number belonging to a third party organisation. Whilst the Royal Bank of Scotland (the "Bank") was informed on repeated occasions, it was evident that faxes were being sent on a regular basis over a significant period of time spanning over 14 months. Although the information contained in the faxes was not sensitive, some did contain customer account information including account number and sort code. The ICO's investigation determined that there was (i) a lack of urgency by the Bank in addressing, managing and recovering the fax disclosures; (ii) there was little action taken by the Bank to contact the unintended recipient for copies of the faxes to investigate the matter further; and (iii) no proactive steps were taken to confirm that the recipient securely destroyed the faxes. Further, despite the Bank sending a communication to all branch staff to raise awareness, the faxes continued to be sent to the incorrect recipient.

The data controller shall, as from the date of this Undertaking and for so long as similar standards are required by the Act or other successor legislation, ensure that personal data are processed in accordance with the Seventh Data Protection Principles in Part I of Schedule 1 to the Act, and in particular that:

1. Procedures are put in place to ensure any reported breach of security relating to personal data is acted upon promptly and any containment and remedial measures are swiftly enforced.
2. Fax procedures are implemented consistently across all branches and regularly monitored to ensure consistent standards. Compliance with any associated fax policy and guidance should be monitored on an ongoing basis and appropriate steps taken to ensure any failings are rectified with minimal delay and by no later than 20 March 2017.
3. To ensure any alternative revised processes are fully tested for security and reliability and any related guidance is disseminated to all staff.
4. Implement such other security measures as it deems appropriate to ensure that personal data is protected against unauthorised and unlawful processing, accidental loss, destruction, and/or damage.

London Borough of Ealing

15 November 2016

DPA – 7th Principle

On 18 February 2016, the ICO was informed by London Borough of Ealing (the "Council") of the loss of a court bundle containing personal and sensitive personal data relating to 27 data subjects including 14 children. A social worker who left Court after attending care proceedings placed an envelope containing the documents on top of her car and drove off. The documents were subsequently lost despite the social worker searching the car park, her route home and making enquiries locally. The Council submitted mitigating factors regarding this incident, stating that training had been completed by the social worker and suitable procedures were in place. However, the ICO's investigations revealed that only 68% of permanent staff had completed refresher data protection training. Further, no records were available relating to the requirements of the Council's 'Paper Records Secure Handling and Transit' policy. This refers to the requirement for a management approval request to be made for removal of documents from the Council's office and that, having been granted consent, document details are entered into in the office log for reference in case of loss. The ICO was also made aware that secure lockable cases had previously been made available but were no longer so.

The data controller shall, as from the date of this Undertaking and for so long as similar standards are required by the Act or other successor legislation, ensure that personal data are processed in accordance with the Seventh Data Protection Principle in Part I of Schedule 1 to the Act, and in particular that:

1. Continue to work toward achieving their stated target for 100% completion of mandatory online data protection refresher training for all permanent, locum and temporary social care staff who handle personal data by 3 April 2017.
2. Record and monitor initial and refresher data protection training for non-permanent staff employed in all other departments of the council involved in the handling of personal data.
3. Ensure that the use of MetaCompliance is a sufficiently robust mechanism for delivering and measuring refresher data protection training to meet the Council's stated objective of an annual requirement.

4. The LBE Management Investigation Recommendations, which are welcomed by the ICO, are progressed as follows:

   a. The review and, ¡f found to be necessary, implementation of an updated Paper Records Secure Handling and Transit Policy is completed by 3 April 2017.

   b. That availability of lockable cases in each area office is completed by 3 April 2017 and that similar arrangements are made in all council departments where removal of similar documents containing personal data from the office is a requirement.

   c. That the review of providing social workers from localities teams with access to mobile working devices when attending court is completed with recommendations made by 3 April 2017.

   d. That the review with the Legal Social Care and Education Department, regarding roles and responsibilities for printing and transporting documents required as part of court bundles, is completed with recommendations made by 3 April 2017.

5. Implement such other security measures as are appropriate to ensure that personal data is protected against unauthorised and unlawful processing, accidental loss, destruction, and/or damage.

Wiltshire Police

9 December 2016

DPA – 7th Principle

A handover file containing officer and witness statements relating to an incident involving imitation firearms and drugs, had been lost. Wiltshire Police (the "Police") understood that this occurred when the file was sent via the Police's internal post. Whilst the officers' statements could be recovered as they had been recorded in the Police's electronic system, the two witness statements had not been filed electronically and therefore could not be recovered. The ICO's investigation revealed that although human error was a factor in this incident, the Police had no record as to whether the staff member involved had data protection training. The Police confirmed that no data protection training records were maintained and that there was no provision of refresher training at the time of the incident.

Undertakings signed in March 2016:

1. Introduce a suitable method of delivering data protection training to all staff who handle personal or sensitive personal data on a regular basis. Attendance/completion of this must be recorded and monitored so that all staff receive the training.

2. Data protection training provided to staff should be refreshed at regular intervals.

3. Deliver appropriate records management training to all staff who are regularly involved with process of files containing personal or sensitive personal data.

4. Monitor the completion of mandatory records management training for such staff and report results into a central location to ensure appropriate oversight of records management training uptake.

5. Implement such other security measures as are appropriate to ensure that personal data is protected against unauthorised and unlawful processing, accidental loss, destruction and/or damage.

Findings of the ICO on December 2016 in relation to undertakings signed:

1. A mandatory online data protection training programme has been developed and is included in the induction programme to be completed by new police officers.
2. In addition to the online training, new police staff will also continue to receive face to face data protection training delivered by the Force Disclosure Unit.
3. A data protection information sheet has been created and is provided to all new starters prior to their start date. The information sheet explains the principles of the Data Protection Act 1998, responsibilities of staff when processing personal data and reporting security breaches. The Police have reported that staff are required to sign to confirm that they have read the information sheet.
4. Existing Police staff are also required to view the online data protection video and complete the online data protection course. An internal email was sent to all staff in July informing them of the mandatory training programme. Since implemented, approximately 800 staff have completed the online training programme.

However, Wiltshire Police should take further action on the following areas:

1. The Police have not yet created a records management training programme to be delivered to staff involved in processing personal and sensitive personal data. The Police have confirmed that there are no plans to deliver records management training to staff. As detailed within the undertaking, appropriate records management training should be delivered to all staff. Completion of records management training should be recorded and monitored.
2. Whilst the Police Learning and Development department maintain a record of staff that have completed the online data protection training package, it remains unclear who is responsible for ensuring mandatory training is refreshed and completed by staff every 2 years.

International Trends

Australia

Overview

The Office of the Australian Privacy Commissioner ("OAIC") has the power to:

- undertake a privacy investigation, whether initiated as a result of a privacy complaint or the Commissioner himself;
- conduct privacy assessments (akin to an audit) of entities;
- make determinations in respect of the above investigations, which may include actions to be taken and/or damages;
- bring proceedings to enforce a determination;
- accept enforceable undertakings from a person or entity;
- bring proceedings to enforce an enforceable undertaking;
- seek an injunction; and
- apply to the court for a civil penalty order.

It is open to the OAIC to use a combination of privacy regulatory powers to address a particular matter.

2016 ENFORCEMENT ACTIVITY

Consistent with the increased interest around privacy, in the 2015-16 financial year (1 July 2015 – 30 June 2016) the OAIC handled 18% more privacy inquiries than the previous year, a total of more than 19,000. However, the rate of privacy inquiries translating into formal complaints lowered.

In the financial year 2015-16, the OAIC:

- handled more than 19,000 privacy inquiries;
- received 2,128 privacy complaints;
- managed 107 voluntary data breach notifications;
- undertook 17 Commissioner-initiated privacy investigations, up from four the previous year;
- conducted 21 assessments of privacy practices of businesses and Government agencies; and
- provided more than 230 pieces of substantial advice to public and private sector organisations.

The most common sectors for privacy complaints and voluntary data breach notifications involved the finance and superannuation sector and the Government sector.

Australia (FY2016)	
Privacy inquiries	19,000+
Privacy complaints	2,128
Voluntary data breach notifications	107
Commissioner-initiated privacy investigations	17 (up from 4 the previous year)
Enforceable undertakings	2
Substantial advice to public and private sector organisations	230+

Most notable actions for 2016

In the past 12 months, the OAIC has made the following three highest determinations for damages:

- On 25 November 2016, the OAIC awarded damages of $10,000 against Veda Advantage Information Services and Solutions Ltd, a credit reporting business, for (i) failure to take reasonable steps to ensure that certain credit information it collected and disclosed about the complainant was accurate, up-to-date, and complete, (ii) using or disclosing credit reporting information that was false or misleading, and (iii) failure to give each recipient of the incorrect information written notice of correction within a reasonable period;
- On 25 November 2016, the OAIC awarded damages of $10,000 against the Commonwealth Bank of Australia Limited for (i) improper disclosure of personal information to third parties, and (ii) failure to take reasonable steps to protect the complainant's personal information from misuse and loss, and from unauthorised access, modification or disclosure; and
- On 27 June 2016, the OAIC awarded damages of $10,000 against a respondent medical doctor for unauthorised disclosure of the complainant's personal information to six individual third parties.

Hot topics / key developments for 2016

In line with international trends, information privacy in Australia garnered significant media and regulatory attention in 2016, and changes to parts of the Australian regulation (including implementation of mandatory data breach notification) appear to be imminent. The Office of the Australian Information Commissioner (OAIC) has been increasingly active in its enforcement of Australian privacy law, and it is anticipated that this will further increase with the implementation of mandatory data breach notification.

Anticipated changes to Australian privacy law

Australia introduces mandatory data breach notification regime

A Bill introducing a mandatory data breach notification regime was passed in February 2017. The regime is expected to come into operation within 12 months and requires agencies and organisations regulated by the Privacy Act to notify the OAIC and affected individuals of an "eligible data breach", which occurs where:

there has been unauthorised access or disclosure of personal information held by the entity and as a result, a reasonable person would conclude is "likely to result in serious harm" to any of the individual(s) to whom the information relates; or

personal information has been lost in circumstances where unauthorised access to or disclosure of personal information is likely to occur, and if it were to occur a "reasonable person" would conclude that it is "likely to result in serious harm" to any of the individuals to which the information relates.

The regulated entity would be required to notify the OAIC and affected individuals as soon as practicable after the entity is aware, or ought reasonably to have been aware, that there are reasonable grounds to believe that there has been an eligible data breach. If an entity suspects an "eligible data breach", the regime will require that entity to carry out an assessment of whether there are reasonable grounds to believe an "eligible data breach" has occurred.

Re-identification of Government data

Another Bill before Parliament is the introduction of a criminal offence where a person re-identifies Government information which has previously been de-identified and made available to the public, or to intentionally disclose this re-identified personal information. The current Bill provides for up to two years in prison or a fine of AUD$21,600 or civil penalty of up to AUD$108,000 for individuals or up to AUD$540,000 for bodies corporate. This amendment is currently being reviewed by a Parliamentary committee and it is unclear if it will be implemented in the proposed form.

Privacy Commissioner v Telstra Corporation

The Full Court of the Federal Court of Australia recently handed down its decision in Privacy Commissioner v Telstra Corporation Limited [2017] FCAFC 4. Prior to its publication, it was expected that this decision would clarify whether metadata is 'personal information' for the purposes of the application of the Australian privacy law. The Full Court did not believe it was necessary to specifically answer this question given the narrow issues before it. As a result, the question of whether metadata is personal information and regulated by the Privacy Act remains open. However, the Full Court found that to be 'personal information' under the Privacy Act, information must be "about an individual", establishing a two-step analysis: (i) is the information about an individual? and (ii) is an individual identified or reasonably identifiable from the information? The Privacy Act applies where the answer to both questions is "yes".

Key Contacts

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

Sylvia Ng
+61 (2) 8266 0338
sylvia.ng@pwc.com

Belgium

Overview

At present, the Belgian Privacy Commission only has 2 executive powers: (i) the power to investigate (on the basis of complaints or on its own initiative) and (ii) the power to demand civil and/or criminal sanctions before court. The criminal sanctions a court can impose include fines up to € 600k, confiscation of the data carriers involved in a privacy violation, the obligatory erasure of data and the prohibition to manage any processing for a 2 year period.

2016 ENFORCEMENT ACTIVITY

BE (2016)	
Monetary Penalties (i.e. fines)	No information available
Undertakings	No information available
Enforcement notices	No information available
Prosecutions	No information available

In 2016, the Belgian Privacy Commission has not taken significant enforcement actions and has not demanded civil and/or criminal sanctions before court. The Commission has concentrated on active collaboration with businesses and actions to raise awareness for online privacy, especially relating to children.

Hot topics / key developments for 2016

Data protection and terrorist attacks in Belgium

Following the terror attacks on the Brussels airport and subway in March 2016, the Belgian Privacy Commission was asked to issue recommendations on passenger name data collection, the exchange of information on 'foreign terrorist fighters' between member states and the ban on the use of anonymous prepaid sim-cards in Belgium. This advice was taken into consideration in several legislative initiatives.

The Facebook case

In 2015, we reported on the ruling of the President of the Brussels Court of First Instance ordering Facebook to cease tracking non-users and stop storing personal data, with the risk of a fixed fine of EUR 250k per day until compliant.

In 2016, Facebook however appealed the case based on grounds of jurisdiction. The Court of Appeal followed Facebook's argument that the case should be referred to the Irish courts, as the main activities of Facebook take place at Facebook Ireland Limited. The Belgian Privacy Commission does not agree and is expected to escalate the case to the Belgian Court of Cassation in 2017.

Draft guidance on the GDPR

In 2016, the Belgian Privacy Commission issued a 13-step plan to inform companies and organizations processing personal data on how to prepare for the implementation of the GDPR.

Furthermore, the Belgian Privacy Commission issued a draft guidance on Data Protection Impact Assessments (DPIA's) under the GDPR. This draft guidance is open to public consultation until end February 2017.

In its draft guidance, the Commission gives more information on the "what, how, when and who" of DPIA's and underlines the importance of a case-by-case analysis to determine whether a DPIA is needed in a specific scenario. The Commission also provides a draft list of some "high risk" cases where a DPIA is in any case mandatory and a draft list of some "low risk" cases where a DPIA is not mandatory.

What to expect for Belgium in 2017?

The Belgian legislator has announced that it will take action in 2017 to implement the GDPR in Belgian legislation. This new Belgian law will amongst others lead to major changes in the functioning and structure of the Belgian Privacy Commission, giving it the muscle and resources it needs.

In the meantime, the Belgian Privacy Commission is already heavily recruiting. We expect the Commission to initiate more investigations and target certain categories of processing or sectors.

The Belgian Privacy Commission is also set to issue more specific guidance on the implementation of GDPR requirements by the second half of 2017, either on its own initiative or through cooperation within the Working Party 29. The Belgian Privacy Commission is expected to remain very active in their collaboration with other DPA's, both on specific cases and within the Working Party 29.

Finally, in 2017, the Belgian Privacy Commission will launch a website especially dedicated and addressed to children and their online privacy.

Key Contacts

Carolyne Vande Vorst
+32 (0) 2 710 9128
carolyne.vande.vorst@lawsquare.be

Leen Van Goethem
+32 (0) 2 710 7876
leen.van.goethem@lawsquare.be

Canada

Overview

The following regulatory enforcement mechanisms are available in Canada:

1. Undertakings
2. Investigations/Audits
3. Monetary Penalties
4. Compliance Agreements
5. Mediations
6. Power to summon witnesses, administer oaths and compel the production of evidence
7. Notice of Violations

2016 ENFORCEMENT ACTIVITY

These statistics are not fully available in Canada; the regulators do not publish all of their annual stats. Below would be an approximation.

CRTC (2016)	
Undertaking	2
Citations	24
Notices of Violations	22

OPC Statistics from Annual report January 1, 2015 – March 31, 2016

PIPEDA complaints accepted	381
PIPEDA complaints closed through early resolution	230
PIPEDA complaints closed through standard investigation	121
Privacy Act complaints accepted and processed for investigation	1,389
Privacy Act complaints accepted and placed in abeyance	379
Privacy Act complaints closed through early resolution	460
Privacy Act complaints closed through standard investigation	766
Public sector audits concluded	1

Most notable actions for 2016

Name of the company subject to fine – Kellogg Canada Inc.

Date fine issued – September 1, 2016

The reason for the fine – In violation of Canada's Anti-Spam Legislation (CASL) Kellogg and/or its third party service providers sent commercial electronic messages (CEMs) to recipients without consent of their recipients. Messages were sent from October 1, 2014 to December 16, 2014, inclusively.

The amount of the fine - $60,000

Industry of the company – Food Processing

Name of the company subject to fine - Blackstone Learning Corp

Date fine issued – October 26, 2016

The reason for the fine – In violation of CASL, Blackstone Learning Corp sent *commercial electronic messages to individuals without consent between* July 4, 2014 and December 3, 2014. During the investigation of alleged complaints, Blackstone Learning Corp *failed to cooperate with the Canadian Radio-television and Telecommunications Commission (CRCT)*.

The amount of the fine – *$50,000*

Industry of the company – Online training/education

Name of the company subject to fine - Sirius XM Canada Inc.

Date fine issued – May 31, 2016

The reason for the fine – Between August 1, 2012 and January 6, 2015 unsolicited telecommunications were made on behalf of SXMC to individuals that were on the 'do not call' list.

The amount of the fine – $650,000

Industry of the company – Broadcasting

Hot topics / key developments for 2016

PIPEDA

PIPEDA is being amended by the Digital Privacy Act with all of the changes expected to come into force in 2017. The key changes include:

a. Data Breach Notifications - Mandatory notifications to the Office of the Privacy Commissioner (OPC) of Canada of any breach of security safeguards involving personal information. For breaches where there is a "real risk of significant harm to individuals," then the requirement also mandates notification to individuals. There is also a mandatory record-keeping for all breaches. Failure to comply could result in fines of up to:

i. $10,000 on summary conviction; and,

ii. $100,000 on indictment.

b. Graduated Consent Standard - An individual's consent will only be valid "if it is reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting."

c. OPC Powers - OPC will be able to form "compliance agreements" with organizations that the OPC has reasonable grounds may have committed, or is about or likely to commit, a breach of the PIPEDA.

d. Disclosure Without Consent – Organizations will be permitted to disclose the personal information without the knowledge or consent of its customers to another organization in order to investigate a breach of an agreement,

contravention, or fraud.

Ontario's Health Information Privacy Law

Ontario's Health Information Privacy Law has been amended in May 2016. Amendments include:

a. Mandatory breach notification to the commissioner of Ontario and to the relevant regulatory college.

b. Double fines for offences of up to $500,000 for organizations, $100,000 for individuals.

c. Extension on 6 months limitation period to prosecute offences.

Ontario's new Privacy Tort

Ontario now has a new tort on the invasion of privacy which resulted from an individual posting a sexually explicit video of his ex-girlfriend on the internet. The Court **recognized liability for "Public Disclosure of Private Facts" and the defendant** paid $100,000 in damages to the plaintiff. The new tort has the following test:

a. the defendant gives publicity to a matter concerning the private life of the plaintiff;

b. the matter publicized, or the act of publication itself, would be highly offensive to a reasonable person; and,

c. the matter publicized, or the act of publication, is not of legitimate concern to the public.

Since coming into force in July of 2014, CASL has been considered the toughest anti-spam law in the world that places strict requirements on (1) sending of any electronic messages ("CEMs") and (2) installing computer programs onto another user's device. CASL continues to evolve with its Private Right of Action coming into force July 1, 2017, and its 3 year review in 2017. Organizations are continuing to struggle with CASL compliance with significant fines that are upwards of $10 million per violation and can include other costs, such as legal fees and reputation damage. Directors, officers and agents can also be held personally liable in the event of a violation. In 2016, several organizations entered into an undertaking with the CRTC, including Kellogg Canada Inc. for $60,000 and Blackstone Learning Corp for $50,000.

Maria Koslunova
+1 (416) 941 8383
maria.koslunova@ca.pwc.com

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

China

2016 ENFORCEMENT ACTIVITY

Year 2016 can be defined as Year 1 of Cybersecurity in China, as the Chinese legislative body adopted the Cybersecurity Law of China and the relevant departments of the Chinese central government also published various administrative rules and regulations regarding each of their specific field for the implementation of the Cybersecurity Law.

Also in 2016 protection of personal information against illegal use, collection and distribution in the public information network gained increasing awareness among the general public in China with several notorious cases involving Baidu, the operator of the Chinese equivalent version of Google, and the major telecommunication operators in China abusing personal information collected in their business leading to serious fraud cases.

Most notable actions for 2016

The Supreme Court of China published on May 9, 2017 a new set of judicial interpretation on the Crimes against Citizen's Personal Information under the Criminal Law of China. This judicial interpretation will take effect on June 1, 2017.

It clarifies on several definitions regarding the Crimes against Citizen's Personal Information: such as what is citizen's personal information and what constitute "illegal obtention" or "illegal provision" of citizen's personal information.

It is noteworthy that the Chinese courts will adopt a quantitive standard, in addition to certain qualitative criteria to the Crimes against Citizen's Personal Information.

	Type of Personal Information	Serious Case	Extremely Serious Case
1	**Location and tracking, content of communication, personal credibility and personal financial information**	More than 50 pieces	More than 500 pieces
2	**Personal information related to accommodation and boarding information, communication record, health and physical information, business transaction, etc.**	More than 500 pieces	More than 5,000 pieces
3	**Other personal information not included in the two types above**	More than 5,000 pieces	More than 50,000 pieces

The judicial interpretation is published in light of the increasingly serious situation of infringement of personal information in China, in particular, in business environment or for purpose of gaining illegal profits.

Hot topics / key developments for 2016

On 7 November 2016, the Standing Committee of the National People's Congress, which is the legislative body of China, adopted the Cybersecurity Law of the People's Republic of China, which was under deliberation by the Standing Committee for more than one year. It demonstrated China's determination to take a more effective and coordinated approach to safeguard the cyberspace as part of China's National Security Initiative.

The proposed law applies to the building, operation, maintenance and use of information networks, and the supervision and administration of cybersecurity in China. In 2015, China also passed the National Security Law and the Law against Terrorism, which, together with this Cybersecurity Law, have demonstrated greater efforts by the Chinese authorities to strength its control over the security of the cyberspace.

Although both domestic and foreign companies will be impacted by the new law, foreign companies doing business in China or with China are more concerned about the impact of the law on them. In particular, companies offering technology and information products, solutions or doing business mainly by using the Internet are more sensitive to the law.

Based on our discussions with some of clients, who are multinational companies, the major three concerns over the new law are:

1. *Restriction on purchase of network products through a government certification system, which may create discrimination against or market access barrier for international companies.*

   On May 2, 2017, The Cybersecurity Administration of China (CAC) published a trial version of the Measures for Security Review of Network Products and Services, which will take effect on June 1, 2017. According to this regulation, network products and services in the financial, telecommunication, energy, public transport, public water conservancy projects and other public utility industries as well as in the e-Government sector will be closely monitored.

2. *Restriction on data transfer overseas.*

   Under the new law, there will be restriction on data transfer overseas for "critical information infrastructure" operators". Such critical information infrastructure will include but not limit to industries such as public communications, information service, energy, transport, water conservancy and utilization, financial service, public service and e-government, and other critical information infrastructure that, once damaged, disabled or data disclosed, may severely threaten the national security, national economy, people's livelihood and public interests.

Overseas transfer of data by such critical information infrastructure operators may be subject to a security review by the Chinese government.

However, the law does not give an exhaustive list of such critical information infrastructure, but rather, it leaves to the State Council, which is the executive branch of the government, to provide detailed rules over the list and the review process. This has created a major concern among international companies which think that they may fall under such a list and thus their free transfer of data may be restricted.

CAC will coordinate with the Ministry of Industry and Information Technology (MIIT) and the Ministry of Public Security (MPS) in publishing the list of the critical information infrastructure. If companies are not clear about their status according to the list, they should consult CAC. Companies that do not fall into the list are not restrained from transferring data outside China; however they are still bound by the obligation vis-a-vis data and privacy protection and the other requirements set by the law regarding data collection, storage, processing and use as well as transfer. If companies fall in the list of critical information infrastructure, they shall submit for security scrutiny before transferring certain data they have collected in China to other countries. CAC published in April 2017 for soliciting public opinion a set of draft rules over Security Review for Outbound Transfer of Personal and Critical Data. It is not known when these rules will be finalized and take effect.

3. *Internet monitoring*.

   Information network or platform 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 warning, fines (on both the business and responsible supervisor(s)) and suspension of business.

The new law will formally enter into force on June 1, 2017. It is estimated that CAC will draft and publish more details rules for implementing the new law before or right after June 1, 2017.

Key Contacts

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

France

2016 ENFORCEMENT ACTIVITY

The French data protection agency, the CNIL, holds its regulatory powers under the French Data Protection Act of 1978. This law was amended by the Digital Republic Law, dating October 7, 2016, which increases the powers of sanctions of the CNIL and entrusts to it new missions. The CNIL may issue to a data controller breaching its obligations, or, where a processing involves the violation of the rights and freedoms of a person, a formal notice of termination of the breach within a time limit.

The CNIL may also issue, after a contradictory procedure (where possible) a warning, an administrative fine, an injunction to cease, or to stop the processing activity. It can order the withdrawal of the processing authorization and lock the access to particular categories of data. As may also carry out on site investigations.

With regards to financial sanctions, the last amendment has increased maximum penalties threshold from 150 000 euros (300 000 euros in case of repeated infringement) to 3 million euros. This harsh increase anticipates on the RGPD which fixes the maximum threshold to a maximum of 4% of the annual turnover for a company. The CNIL may publish the sanctions enacted.

FRANCE (2016)*	
CNIL administrative sanctions	4
CNIL formal warnings	9
CNIL formal notices	82

* Source: CNIL 2016 annual report

Most notable actions for 2016

CNIL / GOOGLE, March 10, 2016:

Since the European Court of Justice ruling of May 13, 2014 which recognized the right to delisting, an 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 the delisting of some results, based on some Google geographical domain extensions (e.g. : .fr, .es, .co.uk; etc…). Such delisting was not applied to generic extensions (e.g.: .com, .net, etc…) or other geographical domain extensions not concerned by the delisting requests (which any internet user may visit alternatively).

Therefore, in May 2015, the CNIL sent Google a formal notice to proceed with the delisting on all of Google's domain name extensions. As Google failed to comply with the CNIL's requirements, the CNIL condemned Google to pay an administrative fine of 100 000 €.

CNIL / MEETIC SAS and SAMADHI, December 15, 2016:

In 2015, following CNIL's on-site inspections, French dating websites companies MEETIC SAS and SAMADHI were put on notice by the CNIL to take actions in order to comply with the French Data Protection Act with regards to the collecting and processing of sensitive data.

Indeed, French law requires that the collecting and processing of sensitive data, such as sexual orientation or ethnicity, are subject to data subjects' express prior consent.

Further to these formal notices, MEETIC SAS and SAMADHI implemented a checkbox notably intended to obtain prior consent for the collecting and processing of the age and sexual orientation data. However, the CNIL considered that such checkbox, which was also used for the user's acceptation of the general terms of the website use, did not enable data subjects to provide a specific and prior consent regarding the processing of their sensitive data.

Therefore, the CNIL condemned MEETIC SAS to pay an administrative fine of 20 000 €, and SAMADHI an administrative fine of 10 000 €.

CNIL / BRANDALLEY, July 7, 2016:

As part of the annual program of the CNIL on-site inspections, French company BRANDALLEY was condemned to pay an administrative fine of 30 000 € on the ground of multiple violations of the French Data Protection Act, in particular, failure to filed prior notification, violation of data conservation legal requirements and failure to collect data subjects' prior consent for the use of internet cookies.

Hot topics / key developments for 2016

A law to prepare for the digital transition

The Digital Republic Law, dating October 7, 2016, amended the French Data Protection Act. Amongst these measures is the obligation for providers *of publicly available electronic communication* services to notify a data breach if there is a risk of infringement of personal data or privacy. The General Data Protection Regulation (GDPR), enforceable in May 2018, compels to the same obligation of notification where there is a violation of personal data. The breach must be reported to the national supervisory authority, in France the CNIL. This law also ensures data portability, which offers the right to transmit directly (where possible) those personal data to another controller without hindrance from the controller who had originally received the data. A right to digital death was adopted, offering the data subject the right to define directives concerning the use of his personal data after his death. Additionally, a specific "right to be forgotten" is created specifically for minors. This provision goes further than the GDPR, which only allows an individual to obtain the deletion of personal data on the internet and the right to object to their data being processed.

A class action for the protection of personal data

The Law on the modernization of justice in the 21st century, dating from November 18, 2016 introduces a class action in the field of personal data. However, this action

only enables to obtain the cessation of the breach, and may not entitle a natural person to obtain compensation for the prejudice arising from the breach.

The creation of a database for identity titles

A Decree published on October 29, 2016 authorizes the creation of a processing of personal data relating to passports and national identity. This information will be gather in a database named "TES" (Secure electronic documents). This database can only be consulted by agents responsible for the management of identity documents such as agents of the Ministry of Interior, anti-terrorist and intelligence services. It may only be used for "authentication" purposes, that is to say, in order to prove a claimed identity. Thus "identification" which consists in finding the identity of a person on the basis of biometric information is not made possible.

New guidance issued by the French Data Protection Authority

Health. The CNIL has adopted on July 21, 2016 two reference methodologies that frame data processing in the field of health research. Whereas the authorization for the processing of research that falls within the scope of these methodologies had to be studied on a case-by-case basis, henceforth the research in question requires only a statement of compliance to the appropriate methodology, and thus, may be implemented 48 hours after the said statement.

Retail & Consumers. A Simplified Standard n°48 issued by the CNIL (The French data protection authority), related to the processing of customers and prospect's personal data, was amended on July 21, 2016. This Standard prohibits telephone solicitation of persons entered on the opposition list, and includes provisions relating to cookies and banking data. It clarifies the notion of the "last contact" from a prospect who is not a client.

Key Contacts

Pauline Darnand
+33 (38) 84 53 261
pauline.darnand@pwcavocats.com

Sandrine Cullaffroz-Jover
+33 (15) 65 74 029
sandrine.cullaffroz-jover@pwcavocats.com

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

Germany

Overview

The German Data Protection Authorities (DPA):

- undertake a privacy investigation, whether initiated as a result of a privacy complaint or the Commissioner himself;
- conduct privacy assessments (akin to an audit) of entities;
- make determinations in respect of the above investigations, which may include actions to be taken and/or damages;
- bring proceedings to enforce a determination;
- accept enforceable undertakings from a person or entity;
- bring proceedings to enforce an enforceable undertaking;
- seek an injunction; and
- order suspensions
- can impose significant fines (up to 300.000 EUR) (which will significantly increase under the new GDPR in March, 2018)

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

Reports: The federal DPAs are obliged to issue "activity reports" regularly (at least every two years), Section 38(1) s. 7 FDPA. Under Article 59 of the upcoming General Data Protection Regulation ("GDPR"), however, each supervisory authority shall draw up an annual report. So far, only Bavaria has issued its complete report (for 2015/2016). However it is likely that many results are exemplary for developments within other German federal states:

Increase of complaints. The Bavarian DPA reports an increase of received complaints in period 2015/2016 (2,527 complaints), compared to the preceding reporting period 2013/2014 (1,878 complaints). New possibilities for addressing complaints online and anonymously might have contributed to that as well as a growth of sensibility and more familiarity with responsible data authorities among the population. 375 of the requests were handed in online last year. Additionally (locally) reworked online forms for complaints have made it easier for authorities to pursue.

Decrease of sanctions. Due to the heavy workload and shortage of personnel, the DPA has been only been able to open sanctioning proceedings in exceptional, severe cases. Thus 173 fine proceedings were actually initiated in 2015/2016. Only 52 of them were concluded with fines.

While the Bavarian authority is keeping a low profile regarding concrete sums of the imposed fines, it is noteworthy, that fine notices have more than halved in 2016, due to insufficient personnel resources. This was partly due to the new requirements of the GDPA, which increasingly demanded personnel attention.

Duration of proceedings before the DPA. (Not only) the Bavarian DPA is confronted by an enormous workload. The authority raised serious concerns on how to meet the forecasted deadlines under the GDPR, in particular the 3 months deadline pursuant to Article 78(2) GDPR. To assess its own capabilities, the (Bavarian) DPA has conducted an internal monitoring of the duration of proceedings administered which, according to the press release, is as follows:

Duration	25%	25%	25%	25%
Complaints	4 days	14 days	52 days	141 days
Consulting citizens	1 day	3 days	11 days	36 days
Consulting companies	3 days	19 days	47 days	122 days

Although new officers shall be hired in 2018, the authority has already proclaimed, that it will not be capable to properly fulfil its responsibilities due to a shortage of personnel.

2016 ENFORCEMENT ACTIVITY

New class action: In February 2016 a German law came into effect which permits consumer protection associations, industry, commerce chambers and other approved business associations to bring "class action"-like claims against businesses and file for injunctions for breach of German data protection law. The new law essentially creates new enforcement possibilities, independent of the authorities of the state. It will strengthen the enforcement of data protection laws in Germany and may potentially result in a wave of collective legal actions due to data protection violations. They also notably affect foreign companies.

Enforcements: a) Safe Harbor Transfers

The companies Unilever, Punica and Adobe have been fined at their German location in Hamburg on basis of unlawfully transferred data from Germany to the US. After the ECJ decision invalidating the Safe Harbor regime, they had missed implementing alternative safeguards for data transfer to the US. During the administrative proceedings initiated by the data protection authorities, the companies implemented the EU Standard Contractual Clauses. Due to these mitigation measures, the fines were significantly reduced from the potential maximum of 300,000 EUR. The companies finally were fined with amounts of 8,000 EUR (Adobe), 9,000 EUR (Punica) and 11,000 EUR (Unilever).

German data protection authorities of Bavaria, Berlin, Bremen, Hamburg, Mecklenburg-Western Pomerania, Lower Saxony, North Rhine-Westphalia, Rhineland-Palatinate, Saarland and Saxony-Anhalt also have conducted investigations of data transfer practices within 500 randomly chosen companies of different sizes and industrial classification on the basis of questionnaires. The outcome has not been published, yet.

b) Intra-group data transfers

Secondly, by an administrative order, the data protection commissioner of Hamburg prohibited Facebook from exchanging user data with its recently bought up company WhatsApp. The instruction was brought up with immediate effect and covered as well the collection as the storing of data. Facebook consequently suspended data exchange of European user data with the parent company in the U.S. but opposed the order, the outcome of which is still pending.

Possible juridical barriers against the approach will be the competence of the Hamburg authority. The authority justified his competence with the data being processed at Facebooks Hamburg office, responsible for marketing affairs. The European court of justice had not accepted this argument in the past referring to the Facebooks European headquarter being in Ireland.

c) Inappropriate Appointment of Data Protection Officer

Finally, another area of published enforcement activities refers to the appointment of a data protection officer. According to the FDPA, companies of more than nine employees equipped with a PC or other data processing measures, must appoint a data protection officer. The Bavarian supervising authority sanctioned the fact that a Bavarian company had appointed its IT-manager as Data Protection Officer. It considered the exposed position of a Manager as inappropriate for fulfilling the tasks as independent data protection supervisor. The company ignored the authority's instructions for months and was punished with a fine, legally binding by now.

Hot Topics / Key Developements for 2016:

It is likely that new developments in the field of data protection will lead to further increase of requests and complaints in Germany. Growing sensibility, easier methods to address complaints and a growing range of persons/ institutions entitled to claim can be seen as key factors. In the same time, a reduction of actually enforced fines was stated, not only in Bavaria. As far as this was caused by the growing workload due to the GDPA, these figures might change in the future. But it is clear that effective enforcement of the newly acquired legal rights can be only accomplished, if adequately supplied by sufficient personnel within the authorities.

It will be interesting to see how the German data protection authorities will change their current practice of imposing rather low fines under the upcoming GDPR, which provides for a much stricter enforcement regime.

Key Contacts

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

India

Overview

There are various regulatory bodies with powers for enforcement of the respective Act and regulations.

IT Act 2000

The Adjudicating officer under the IT Act has powers to:

- Holding an enquiry in the manner prescribed by the Central Government
- To impose such penalty or award such compensation as he thinks fit in accordance with the provisions of that section
- Shall have the powers of a civil court which are conferred on the Cyber Appellate tribunal under sub-section (2) of section 58, and –
  - All proceedings before it shall be deemed to be judicial proceedings within the meaning of sections 193 and 228 of the Indian penal Code
  - Shall be deemed to be a civil court for the purposes of sections 345 and 346 of the Code of Criminal Procedure, 1973

While adjudicating the quantum of compensation, the adjudicating officer shall have due regard to the following factors, namely

- The amount of gain of unfair advantage, wherever quantifiable, made as a result of the default
- The amount of loss caused to any person as a result of the default
- The repetitive nature of the default

2016 IT Act enforcement activity

This information is not available in the public domain

Department of Telecommunications – Amendment to Access Service License agreement

Department of Telecommunications (DOT) has the following powers:

- To conduct an audit of the telecommunication service provider.
- To levy a penalty - Section ix) a) A penalty of Rs 50 crores will be levied for any security breach which has been caused due to inadvertent inadequacy/ inadequacies in precaution on the part of licensee prescribed under this amendment.
- To initiate legal proceedings - Section ix) c) Besides the penalty, liability and criminal proceedings under the relevant provisions of various Acts such as Indian Telegraph Act, Information Technology Act, Indian Penal Code (IPC), Criminal Procedure Code (Cr PC) etc. can be initiated.

2016 ENFORCEMENT ACTIVITY

This information is not available in the public domain

Unique Identification Authority of India (UIDAI) - Aadhaar Act, 2016

The authority has the following powers under the Act:

No court shall take cognizance of any offence punishable under this Act, save on a complaint made by the Authority or any officer or person authorised by it.

No court inferior to that of a Chief Metropolitan Magistrate or a Chief Judicial Magistrate shall try any offence punishable under this Act.

Notwithstanding anything contained in the Code of Criminal Procedure, 1973, a police officer not below the rank of Inspector of Police shall investigate any offence under this Act.

Most notable actions of 2016

31-January 2017

UIDAI shuts down 24 unauthorized websites and mobile applications providing illegal services in the name of UIDAI/ Aadhaar and collecting personal details of the residents.

23-February 2017

UIDAI filed criminal complaint against 3 large companies for allegedly storing biometrics and using them in an unauthorized manner in violation to the Aadhaar Act, 2016.

28-February 2017

UIDAI filed an FIR against a person for allegedly spreading rumours on internet about the vulnerability and weakness of UIDAI system

27-March 2017

UIDAI files an FIR for receiving two Aadhaar applications with different names but the same biometric information was registered.

Hot topics / key developments for 2016

Notification of Aadhaar Act 2016 and Aadhaar Regulations 2016

The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 gives statutory backing for the unique Aadhaar number to be used as proof of identity for accessing services such as bank accounts and phone connections, or for disbursal of subsidies and government benefits.

The Aadhaar initiative was launched in 2009 to provide everyone in India with a unique identification number (UID). Aadhaar is world's largest biometric identification programme with over 100 crore registrants.

Important Privacy Provisions

- 8(2) Obtain the consent of an individual before collecting his identity information for the purposes of authentication; ensure that the identity information of an individual is only used for submission to the Central Identities Data Repository for authentication.
- 8(3): Inform the individual submitting his identity information for authentication- about the nature of information that may be shared upon authentication; the uses to which the information received during authentication may be put by the requesting entity; and alternatives to submission of identity information to the requesting entity
- 29(1): No core biometric information, collected or created shall be shared with anyone for any reason whatsoever; or used for any purpose other than generation of Aadhaar numbers and authentication.
- 29(2): The identity information other than core biometric information, collected or created under the Act may be shared only in accordance with the provisions of the Act.
- 29(3): No identity information available with a requesting entity shall be used for any purpose, other than that specified to the individual at the time of submitting any identity information for authentication; or disclosed further, except with the prior consent of the individual to whom such information relates.
- 29(4): No Aadhaar number or core biometric information collected or created under this Act in respect of an Aadhaar number holder shall be published, displayed or posted publicly, except for the purposes as may be specified by regulations.
- 57: Nothing contained in the Aadhaar Act shall prevent the use of Aadhaar number for establishing the identity of an individual for any purpose, whether by the State or any body corporate or person, pursuant to any law, for the time being in force, or any contract to this effect provided that the use of Aadhaar number shall be subject to the procedure and obligations under the Aadhaar Act.

The authority has recently notified the regulations under the Aadhaar Act covering areas of Sharing of Information, Data Security, Authentication, Enrolment and Update, Transaction of Business at Meetings of the Authority.

Penalty and punishment

Sections 40, 41 and 42 of the act deal with penalties and punishment for offending entities.

Unauthorised use or unauthorised sharing of information will attract imprisonment up to three years and a fine that may extend to 10,000 INR (or 1,00,000 INR in the case of a company).

Failing to intimate customers about the purpose of the collection of information, or failing to obtain user consent for authentication, or failing to meet other provisions of the law will attract imprisonment up to one year and fine that may extend to 10,000 INR (or 1,00,000 INR in the case of a company).

Section 43(1) identifies people to be held responsible in case the offending entity is a company. In such a scenario, everyone in-charge of the company and everyone responsible to run the business of the company will be deemed guilty.

Cyber Security framework in Banks, June 2016 by Reserve Bank of India (RBI)

RBI has come up with a Cyber Security framework for Banks to enhance the current defences of the Banking system to address the cyber risks.

The important provisions of the framework are Cyber security policy, continuous surveillance, IT architecture, network and database security, protection of customer information, Cyber crisis management plan, Cyber security preparedness indicators, Sharing of information on cyber-security incidents with RBI, Supervisory reporting framework, immediate assessment of gaps to be reported to RBI, Organisational arrangements, cyber security awareness among stakeholders/Top Management/ Board, Baseline Cyber security and Resilience requirements, C-SOC (Cyber security operation center)

Key Contacts

Rajinder Singh
DSCI Certified Privacy professional (DCPP), CIPP/US
+91 9873264886
rajinder.singh@in.pwc.com

Faiz Haque
DSCI Certified Privacy Professional (DCPP)
+91 8130064263
faiz.haque@in.pwc.com

Italy

Overview

The Italian Data Protection Code attributes to the Data Protection Authority (IDPA) several enforcement mechanisms to be used in order to ensure that the personal data are processed by companies and individuals in accordance to the data protection legislation.

First of all, the IDPA's main role is to verify whether the data processing operations are carried out in compliance with the laws and regulations in force. For such purpose, the IDPA may either: (i) order data controllers or processors to adopt the measures deemed necessary or appropriate for the processing to be compliant with the law provisions; (ii) prohibit unlawful or unfair data processing operations, in whole or in part; or (iii) block those processing operations that are carried out in violation of the law provisions.

In addition, the Data Protection Code acknowledges to the IDPA a general power to inquire and control. In particular, pursuant to Section 157 of the Italian Data Protection Code, the IDPA can request the data controller, data processor, the data subject or a third party to provide information and to produce documents. Furthermore, the IDPA may order to access databases and filing systems or to perform audits in the premises where the data are processed or to carry out investigations.

The main enforcement mechanism provided by the Data Protection Code to the IDPA is the power to apply sanctions in the event of a violation of the privacy rules. Pursuant to Sections 161 and following of the Data Protection Code, non-compliance to data protection law can be punished either with criminal or administrative sanctions, even though, to our knowledge, as of today in Italy criminal sanctions have never been applied with respect to offences regarding the violation of the data protection legislation.

With reference to the administrative sanctions, the applicable fines provided under the Data Protection Code range from a minimum of €1,000 to a maximum of €180,000. The highest sanction can be imposed by the IDPA, pursuant to Section 162, paragraph 2-ter, of the Code, in the event of non-compliance to the recommendations made by the IDPA, either setting out to the data controller or processor necessary measures to be undertaken/implemented or prohibiting the further processing of personal data in the event of a violation.

In any case, in Italy the amount of the applicable sanctions can vary significantly if the violation refers to less serious cases or aggravating circumstances. As a matter of fact, if the violation is considered by the IDPA less serious, also with regard to the social and/or business features of the activities at issue, the upper and lower thresholds set forth shall be reduced by two-fifths. At the same time, however, if one or more provisions are repeatedly violated, also on different occasions, in connection with large databases, the sanction can rise up to €300,000 and is not allowed to be reduced. Finally, if the prejudicial effects produced on one or more data subjects are more substantial or if the violation concerns several data subjects, the upper and lower thresholds of the applicable fines shall be doubled.

2016 ENFORCEMENT ACTIVITY

Italy (2016)	
Sanctions	2,339
Report to the Judicial Authority	53
Provisions regarding security measures	26
Fines collected as of March 2017	3,300,000

The sanctions applied mainly relate to data breaches, insufficient information provided to the data subjects with respect to the processing of personal data, storage of phone and web data for longer periods than those allowed, as well as omitted notification to the Authority when required by the Data Protection Code with respect to particularly sensitive processing of personal data.

The IDPA each year in June issues an Annual Report with the indication of the main activities performed and the decisions taken in the previous year. Therefore, in June 2017 a summary of the main sanctions applied during 2016 will be available on the Authority's website for public consultation. Until the release of the mentioned document, it is possible only to provide an indication of the sanctions applied.

In any case, in September 2016 and March 2017, the IDPA released a Newsletter that analysed the enforcement trends of the first semester of the year, as well as provided an estimate of the area of investigation for the second semester. In particular, the main areas on which the IDPA focused its investigative activities during such period concerned (i) big public databases (i.e. the Italian social security agency and the Italian tax agency); (ii) the transfer of personal data by multinational corporations; (iii) web marketing and telemarketing activities; (iv) technical assistance for data recovery within personal computers or mobile phones; (v) genetic research activities; (vi) car sharing companies. With respect to the second semester of 2016, the IDPA focused its activity on telemarketing companies, call centres, entities helping employees with the individual income tax return, as well as online games dealerships.

Most notable actions for 2016

We do not have access to all the sanctions issued by the IDPA in 2016. However, among those that we are aware of, the highest fine issued, on March 31, 2016, was of €192,000. In particular, the sanction was applied by the IDPA to a lawyer that stored a large database with illegally acquired personal data (also judiciary data) and phone numbers, without having duly informed the data subjects and obtained their prior consent.

A milestone decision has been adopted in February 2017 by the IDPA which applied an overall administrative sanction of 11,000,000 towards 5 companies operating in the money transfer sector. In particular, the companies used to collect and transfer money to China by splitting up the amounts and attributing them to unaware clients, without their prior

consent, in order to hide the identity of the real senders.

Hot topics / key developments for 2016

In 2016 the IDPA issued the rules for the proper use of data regarding the reliability of entrepreneurs and managers. In the words of the IDPA, this is a very sensitive area for the proper functioning of the market and an incorrect use of databases and other analysis tools can cause serious damage to the dignity and privacy of the people involved.

On October 1, 2016 the Code of Ethics and Conduct in Processing Personal Data for Business Information Purposes entered into force.

According to the Code of Ethics, companies offering information on the commercial reliability of entrepreneurs can collect data without the prior consent of the data subject: (i) from public sources, in the meaning of public registers, lists, instruments or records that are publicly accessible (i.e. financial statements or any other record from the Chamber of Commerce); (ii) from publicly and generally accessible sources, such as newspapers, business or phone directories, public entities' or authorities' websites; (iii) directly from the data subject.

If the company's annual turnover relating to business information services exceeds €300,000 it shall join a shared portal where to place communications on commercial information (www.informativaprivacyancic.it), otherwise, the company shall make available to the data subject through its own website a proper and complete information notice. In addition, there is a general obligation to provide the data subject with a prompt reply in case of requests of access to their personal data.

Data collected for business information services can only be stored for as long as it remains accessible and/or is published in the respective public source pursuant to the applicable sector-specific legislation and shall be protected with proper security measures in order to guarantee their integrity.

Key Contacts

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

Flavia Messina
+39 (02) 916 05 054
flavia.messina@it.pwc.com

Japan

Overview

Japan implemented the "MyNumber" system in early 2016, based on the Act on the Use of Numbers, to Identify a Specific Individual in the Administrative Procedure (MyNumber Act), and the Act on the Protection of Personal Information (Personal Information Protection Act: PIPA). The MyNumber system assigns an individual number to all residents of Japan, to harmonise administrative procedures among government agencies and also to prevent crimes such as tax evasion and fraudulent welfare claims.

MyNumber System (The Social Security and Tax Number System)

The MyNumber system requires all companies to handle individuals' MyNumber in accordance with the requirements set out in the Act, which includes specific measures around handling procedures of individuals' MyNumber. Since individuals' MyNumbers are classified as Specific Individual Information (SII) they require special care for handling and attract higher penalties for mishandling than the current PIPA. According to Article 67 of the MyNumber Act, disclosing SII, including individuals' MyNumber, to any third party without legitimate reason or consent can result in up to 4 year's imprisonment, a fine of up to ¥2M, or both.

Personal Information Protection Act

Under the PIPA article 74, the loss of personal information through negligence or an otherwise lack of care of duty can result in up to 3 month's imprisonment or a fine of up to ¥300k. These penalties, however, have not been enforced since the enactment of the PIPA in 2005.

Amended Personal Information Protection Act (effective May 2017)

The enforcement clauses of the amended PIPA are to be strengthened compared to the current PIPA. Article 83 of the act, allows for imprisonment of up to 1 year or a fine of up to ¥500k for individuals responsible for the unauthorised disclosure of personal information. Additionally, Article 87 states a fine of up to ¥500k for the responsible individual's company.

2016 ENFORCEMENT ACTIVITY

As mentioned in Answer 1, there have been no enforcement action taken in 2016 with regards to PIPA.

Hot topics / key developments for 2016

On December 20, 2016, it was determined by the Japanese cabinet council that the amended PIPA will be put into full effect on May 30, 2017.

The amended PIPA, includes the below additions;

- Biometric information which can be linked to a specific individual (e.g. through passport number, license number, residential code) are defined as "individual identification codes".
- A person's race, religious beliefs, social status, medical history, criminal records, etc. are defined as "sensitive personal information" which requires special consideration in handling, such as obtaining explicit consent from the information subject prior to transferring.
- The scope of the amended PIPA is extended to companies handling the personal information of less than 5,000 subjects, which were previously exempt from the former PIPA.
- When personal data is provided to a third party, the provider and recipient must confirm and record the rationale for the data transfer.
- New terminology - "de-identified information" - was introduced for anonymised information which cannot be de-anonymised through reverse engineering. The amended measures in the PIPA are not applicable to this de-identified information, and companies are free to use this information for various purposes.
- The requirements for firms to be able to provide data subjects with the opportunity to "opt-out" of data privacy regulation protection has been strengthened. From March, companies wishing to request data subjects to "opt out" must register with the Personal Information Protection Commission.

When the PIPA was first enacted in 2005 it drew much attention and concern from businesses, and awareness of privacy has only increased ever since – this is reflected in the newly defined laws and regulations. Japan's Personal Information Protection Commission has also issued various practical guidelines for these areas.

As Japanese companies increasingly seek their future growth beyond their domestic market, they are also finding themselves subject to overseas laws and regulations in relation to Data Privacy, such as GDPR in EU and Cyber Security Law in China. The amended PIPA includes various clauses similar to the legislation in other countries so companies aligning to the amended PIPA may be able to leverage this effort for compliance with other overseas data privacy legislations, although potential gaps must be considered.

Key Contacts

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

Mexico

Overview

The National Institute of Transparency, Access to Public Information and Data Protection (INAI) has the power to:

- Monitor and verify that the provisions of the Federal Data Protection Law (LFPDPPP) are being complied by individuals or corporations processing personal data, carrying out investigations requested by data subjects or INAI itself (data protection procedure, verification procedure, penalty procedure)
- Make determinations in respect of the above investigations, which may include actions to be taken and/or penalties.
- Apply to court for criminal judgement.

Infringements to the Law will be punished by INAI with fines from 100 to 320,000 days of the General Current Minimum Wage in Mexico (MXP$80.04)

- Regarding infringements committed in processing sensitive personal data, sanctions may be doubled.
- INAI will ground its decisions in law and fact, considering:
- The nature of the personal data concerned,
- The evident inappropriate 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,
- Recurrence.

The Law also considers crimes related to unlawful processing of personal data:

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

With regard to sensitive personal data, the penalties referred will be doubled.

2016 ENFORCEMENT ACTIVITY

During 2016, INAI handled 444 privacy inquiries:

- Received 92 verification procedures;
- Received 143 data protection procedures;
- Received 32 penalty procedures;
- Managed 177 of other type of procedures (i.e. guidance to private and public sector);
- Penalties increased in the amount of $7'576,160.80 pesos compared to 2015;
- managed 107 voluntary data breach notifications;

Most notable actions for 2016

The penalties applied by INAI during 2016 in 53 resolved cases are for the total amount of $93'000,135.88 pesos. Up to this moment there is no specific information published of each case.

Hot topics / key developments for 2016

On May 9th, 2016 the Federal Law of Transparency and Access to Public Information was published. It has as main purpose to ensure an adequate level of protection to the processing of personal data and public information held by Legislative, Executive and Judicial powers, as well as the protection of all personal data collected and processed by governmental institutions. Data protection by public institutions was not as well-regulated as it is now with these new legal provisions.

Key Contacts

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

Netherlands

Overview

In the Netherlands the Data Protection Authority (in Dutch: Autoriteit Persoonsgegevens (AP)) is responsible for the enforcement of data and privacy protection laws. As per the 25th of May 2018, with the introduction of the European General Data Protection Regulation (GDPR), the powers of the AP will be expanded. Under current law the AP has the following powers:

- Undertaking investigations assessing compliance with the law. In case of a violation of the law or of the regulations based on the law, the Dutch DPA can use its (administrative) enforcement powers, for example by issuing an order to cooperate or by issuing a conditional fine.
- Conducting preliminary examinations to assess the legitimacy of certain processing operations that involve specific risks.
- Assessing codes of conduct for specific sectors relating to the processing of personal data.
- Mediating in disputes regarding the exercise of rights and undertaking investigations to assess compliance with the law or of regulations based on the law, at the request of an interested party. Please note that each time a request for mediation or a complaint is received, the Dutch DPA checks whether the request or complaint fulfils the statutory requirements and whether there is sufficient reason to take it up.
- Keeping a public register of notifications of processing operations. Pursuant to the Dutch Data Protection Act, organisations must notify the Dutch DPA of the processing of personal data, unless the processing operations have been exempted from the notification obligation. The notifications ensure openness with regard to the processing of personal data by controllers.
- Assessing requests for granting exemptions from the prohibition to process sensitive data.

As from the 25th of May, 2018 (under the GDPR), the following powers will be added:

- In order to improve the investigative powers, the AP may carry out data protection audits, during which the AP has the right to obtain all personal data and information necessary and to obtain access to any premise, including date processing equipment.
- The correctional powers of the AP will be strengthened with several measurers from reprimands and warnings to ordering temporary limitations and total bans of processing or the suspension of data flows to third countries.
- The maximum fine for none compliance will be raised from €820.000 to €20 million or 4% of the worldwide turnover, whichever is higher.

2016 ENFORCEMENT ACTIVITY

Since 1 January 2016, the Dutch Data breach notification act has entered into force. The total number of data breach notification is lower than was previously expected. No fines have been issued yet, but it is expected that the first penalties will be announced shortly, as some data breaches are still under investigation. The chairman of the AP has announced that the first penalties with respect to data breaches will follow.

In the financial year 2015-16, the AP:

- handled a number of approximately 5,500 data breach notifications;
- of which 4,000 have been subject to initial research of the AP;
- in a number of +/- 100 cases the AP has issued a warning;
- A few dozen of cases are still under investigation (exact number unknown).

The Netherlands (FY2016)	
Data breach notifications	+/- 5,500
Data breaches investigated by AP	+/- 4,000
Issued warnings	+/- 100
Data breaches under further investigation, penalty may be issued	+/- 20-100

Most notable actions for 2016

The AP has not yet issued (unconditional) fines. The following are the three key examples of execution of the monitoring powers of the AP:

- On July 7, 2016, the AP published a research report on the screening at Hoffmann Bedrijfsrecherche B.V., a business investigation company. In the year 2016 the AP focused on the processing of data resulting from the relationship between employee and employer. The AP suspected that the company lacked a lawful basis for the processing of data, obtained through screening of job applicants. The company has changed its methods in co-operation with the AP in order to comply with the law, so no fines were imposed.
- On June 20, 2016, the AP imposed a conditional penalty payment of €5000 a week on Bluetrace B.V., a company that used a WIFI-tracking app to monitor the shopping behaviour of people in and around shops, if they would continue tracking without consent. The decision was based on a research report by the AP.
- In 2016 the AP started an investigation on the drug and alcohol testing of employees at Uniper Benelux N.V. The AP started the investigation after complaints by employees. The AP found that employees were not free to decline a drugs test and therefore couldn't give their free consent. As this was the basis for the processing of personal data resulting from the tests, the tests were deemed illegal. During the investigation Uniper stopped this practice, resulting in no further measures being taken by the AP.

Hot topics / Key Developements for 2016:

GDPR implementation legislation us under construction

As the GDPR has direct effect, the direct working articles will not be converted into Dutch national legislation. On a number of points additional national legislation is required. This concerns, in short, the following:

1. The implementation of the provisions regarding the national regulator; and
2. Elaboration of the discretionary space left to the member states on certain GDPR provisions (e.g. specific national regulations regarding genetic information or exceptions for scientific research)

For these topics, the Dutch legislator will choose for a so-called policy neutral implementation. This means that existing law will be maintained, unless this is not possible in the light of the regulation.

Privacy Governance Survey

Over the past years more than 200 organisations in the Netherlands have participated in the PwC Privacy Governance Survey. The Privacy Governance survey provides an overall insight into how Dutch organisations deal with privacy, why they believe it is important, and how they deal with current and new data privacy regulations. The Privacy Governance Survey provides a unique insight in Dutch organisations' readiness for the GDPR and their level of maturity in dealing with the protection of personal data. It also enables organisations to compare their results with other relevant organisations.

Last year's results of the Privacy Governance Survey show important the proportion of organisations that are fully prepared for the data breach notification obligations rose from 16% to 58%. This is reflected in the fact that within 70% of the organisations (in 2015 just 50%) intensive cooperation between Legal, IT (security) and Business is taking place with regard to privacy and data protection. At 74% of the organisations (against 50% in 2015) increased investments in privacy compliance took place. Also the upcoming enforcement of the GDPR has contributed to increased attention to privacy and processing of personal data. This is supported by the fact that almost 90% of the participants stated that they have a good insight in the personal data processing within their own organisation, as compared to only 68% last year.

For more detailed results of the Privacy Governance Survey a copy of the report can be downloaded at www.pwc.nl/nl/digital/privacy.

Key Contacts

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

New Zealand

Overview

There are no immediate enforcement mechanisms available to the Office of the Privacy Commissioner in NZ. Complaints can be made to the OPC by anyone who believes they have been subjected to an "interference with privacy" and they have broad powers to enquire into any matter if they believe the privacy of an individual is being infringed. If they find cause they can mediate or refer to the case to the Director of Human Rights Proceedings who can take legal action.

2016 ENFORCEMENT ACTIVITY

In the year to 30 June 2016 (the statutory reporting period for the OPC) there were 940 complaints, 461 were closed through settlement (either by information release or correction, apology, monetary, assurances, changes of policy, or training). More detailed statistics are not available. Of these 2 were referred to the Director of Human Rights Proceedings for further action and 34 matters were raised directly with the Director of Human Rights Proceedings separate to the OPC.

During 2016 13 case notes were published by the OPC. These had the following outcomes:

NZ Cases (2016)	
Referred to Director of Human Rights Proceedings	2
Settlement or compensation	6
Formal apology	4
Information released to individual (in whole or in part)	2
Information deleted or corrected	4
Offending organisation policies or processes changed	4
Offending organisation publicly named	1
No breach found	2

A further 9 decisions were made by the Human Rights Review Tribunal where action was taken by the Director of Human Rights Proceedings relating to the Privacy Act 1993. Of these 4 were found to have no breach, 1 was found to have non-compliance but no harm so no damages were awarded, 3 were deferred to separate or future cases, and 1 resulted in a formal apology and settlement.

Most notable enforcement action in 2016

Fines are not issued under NZ legislation and information on settlements is not generally released publicly. The information to answer this question is not available.

Hot topics / key developments for 2016

- Areas of inquiry undertaken by the Office of the Privacy Commissioner in 2016:
  - Spot checks on credit reporter compliance with the Privacy Act and Credit Reporting Privacy Code – noted instances of failing to respond to access requests, some slow responses and one reporting without all expected information
  - Privacy and Online Property Information – a number of complaints have been made historically about information being published by government (local and central) – this report provides guidance to local authorities
  - Transparency Reporting Trial – indicating the number of government made requests for personal information from other agencies or organisations
- A new process was developed to provide advisory opinions - intended to promote understanding of the information privacy principles and give greater certainty to Ministers and agencies in relation to the Act's operation in particular circumstances
- Proposed code amended to better facilitate emergency responses
- Review of credit reporting law launched

Key Contacts

Drew Parker
+64 (4) 462 7104
drew.x.parker@nz.pwc.com

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

Norway

Overview

In Norway the Norwegian Data Protection Authority has the responsibility to enforce the Personal Data Act and the Personal Data Regulations. The Data Protection Authority protects the right to privacy and strives to prevent misuse of personal data. They shall

- keep a systematic, public record of all processing that is reported or for which a licence has been granted
- deal with applications for licences, receive notifications and assess whether orders shall be made in cases where this is authorized by law
- verify that statutes and regulations which apply to the processing of personal data are complied with, and that errors or deficiencies are rectified
- keep itself informed of and provide information on general national and international developments in the processing of personal data and on the problems related to such processing
- identify risks to protection of privacy, and provide advice on ways of avoiding or limiting such risks
- provide advice and guidance in matters relating to protection of privacy and the protection of personal data to persons who are planning to process personal data or develop systems for such processing, including assistance in drawing up codes of conduct for various sectors
- on request or on its own initiative give its opinion on matters relating to the processing of personal data

The Privacy Protection Committee is the appeal body for decisions made by the Norwegian Data Protection Authority. The Privacy Protection Committee shall consider complaints on decisions made by the Norwegian Data Protection Authority. The Committee has seven members, appointed for four years with possibility of four more years.

2016 ENFORCEMENT ACTIVITY

The Norwegian Data Protection Authority conducted a total of 86 inspections i 2016. Most of them concluded with some kind of defect, but none resulted in monetary penalties.

Most notable enforcement action in 2016

None of the inspections conducted in 2016 resulted in monetary penalties.

Hot topics / key developments for 2016

GDPR was a main topic for the Data Protection Authority, and amongst other things they have provided guidance on the new regulation.

Digitalisation of public sector is a focus area in Norway. ICT is essential to achieve simplification and efficiency in the Norwegian public sector. When multiple services is available online, this gives new privacy-related challenges, and also providing opportunities to build privacy considerations into solutions.

The healthcare and welfare sector is subject to major changes and the changes are happening at a fast pace. Both when it comes to new legislation and the developments in e-health.

In the justice sector, we meet weighty considerations in favor of the state to intervene in individual's privacy. Often this happens without the individual's participation and with limited right to information. Individuals thus have opportunities to safeguard their interests. In these areas it is particularly important for the national regulatory authorities to ensure that the individual's rights are protected.

Key Contacts

Lars Erik Fjørtoft
+47 (0) 974 74 469
lars. Fjørtoft@pwc.com

Line Marie Engebretsen
+47 (0) 982 14 600
line.engebretsen@pwc.com

Poland

Type of action	2016	2015	2014
Complaints	2610	2256	2472
Inspections	192	175	175
Data filing systems registrations	6799	10737	16870
Motions for registering data filing systems	30479	31501	43300

Overview

The Office of the Polish data protection authority (the General Inspector of Personal Data Protection, GIODO) has the power to:

1. supervise ensuring the compliance of data processing with the provisions on the protection of personal data,
2. issue administrative decisions and consider complaints with respect to the enforcement of the provisions on the protection of personal data,
3. impose enforcement financial penalties for non-fulfillment of non-pecuniary obligations arising under the decisions referred to in point 2 above,
4. keep the register of data filing systems and the register of administrators of information security, as well as provide information on the registered data files and the registered administrators of information security,
5. issue opinions on bills and regulations with respect to the protection of personal data,
6. initiate and undertake activities to improve the protection of personal data,
7. participate in the work of international organizations and institutions involved in personal data protection.

2016 ENFORCEMENT ACTIVITY

In 2016 Polish personal data protection authority received 2610 complaints from data subjects regarding their personal data being wrongfully or unlawfully processed. In comparison to preceding years, the number of complaints increased (2015 – approx. 2200 complaints, 2014 – approx. 2500 complaints, 2013 - approx. 1900 complaints and 2012 - approx. 1600 complaints).

In 2016, GIODO registered 6799 data filing systems. Such amount should be considered a significant decrease, especially compared to approx. 10,700 registered data filing systems in 2015 and approx. 16,900 in 2014. It is worth noting that the number of motions for the data filing systems registration has not dropped accordingly. In 2016 almost 30,500 motions were filed compared to approximately 31,500 motions in 2015.

Most notable actions in 2016

The most interesting decisions of GIODO issued in 2016 are summarized below.

- Registration of pre-paid sim cards

Under new antiterrorist laws in Poland, telecommunication operators are obligated to register all pre-paid sim cards used in cell phones in order to identify sim card's owner. Such registration requires identification of an individual whose personal data are needed to be memorized in operator's databases. In practice, telecommunication operators were asking individuals to provide their ID cards which were then copied. Such practice was questioned by the data protection authority.

Polish law allows telecommunication operators to process all data included in copies of documents confirming ability of an end user to execute his/her obligations under a telecommunication service agreement. GIODO considered that this right of the operators is strictly related to processing the personal data for the purposes of entering into such agreements. For the purposes of registering pre-paid sim card, copying all personal data from individuals' IDs requires data subject's consent (decision No. DIS/DEC-218/16/19879).

Such consent should be provided voluntarily. GIODO reminded that the law prohibits operators to make dependant the conclusion of a service agreement from providing data and information in a scope more extensive than legally required (decision No. DIS/DEC-170/16/14463).

- Separating consent clauses

Online activity of an end-user often requires granting consent to personal data processing. When consent is collected to personal data processing for marketing purposes, it is necessary to give a choice to a data subject as to granting such consent to selected data controllers.

One of companies located in Poland has started an interesting online business which was thought to create a database of addresses (locations) where courier / post parcels are usually delivered easily or there are problems which such a delivery. The database was to be created by the end-users themselves (they were filling in the database with information coming from their delivery experience). For the purposes of the use of the online service, the end users were asked to consent to their personal data processing for marketing purposes. The consent included not only the service provider but also other companies – partners of the service provider.

GIODO stated that consent clauses should be separated: one clause should be for receiving commercial information from the service provider, a separate one – for receiving commercial information from partners of the service provider, and another one – for sending information by the service provider about the service itself (e.g. about technical issues related to the service). Only such separation of consent clauses allows for providing voluntary character of granting consent

for marketing purposes (decision No. DIS/DEC-4/16/684).

Interestingly, GIODO also stated that information about address of a building (location) combined with information about successful / unsuccessful delivery of a parcel to such an address, may – in certain situations – constitute personal data.

Establishment of a data controller

The Polish data protection authority has added its voice into a discussion on EU member states jurisdiction over social media providers which have their main seat in the USA and carry out business activity in the context of establishment in EU member states (see: European Court of Justice decision C-131/12, Belgian court (Brussels Court of Appeal) decision dated 28 June 2016).

In short, personal data (including address, ID card number) of an individual were mentioned in criminal records, which were published on Facebook portal. In its decision issued in January 2016 (DOLiS/Dec-50/16) the Polish data protection authority ordered a data controller to remove all such personal data. To enforce complete erasure of such data from the online service, GIODO addressed its decision towards Facebook Poland (although the company declared that the data controller is the Irish subsidiary of Facebook). GIODO based its decision and its addressing on the idea of an establishment of a data controller included in provisions of the EU directive 95/46/EC and their interpretation done by EU Court of Justice in the case no. C-131/12.

GIODO stated that the activity of Facebook in Poland was in reality a continuation of the activity of Facebook Inc. Moreover, GIODO stated that even though Privacy Policy of the social media portal indicated that the data controller is the Irish subsidiary of Facebook, the analysis of its provisions led to a conclusion that it is Facebook Inc. that decides on rules of personal data processing. As result, the activity of the Polish subsidiary of Facebook was said to be an establishment which requires fulfilling personal data protection requirements.

Hot topics / key developments for 2016

Concept of one collective data controller

New widely discussed and controversial act was implemented in Polish law, which in general guaranteed parents monthly payment for kids. The payment of such parental benefit is strictly connected with processing of benefiters' data by authorities. There are many authorities which have access to personal data of benefiters in relation to the payment of the parental benefit. To make exchange of such personal data easier for the authorities, Polish legislator came up with a unique concept of a "collective data controller".

Under the new law, public bodies are treated as one data controller (and not joint controllers) if the processing of personal data by them is done for common purpose (in public interest). The concept of one "collective data controller" is not known under EU law (directive 95/46/EC or General Data Protection Regulation - GDPR). Consequences of such a concept are difficult to predict, just to mention realization of notification obligation (which authority should a request for information be direct it to?) or entrusting data processors with processing of personal data on behalf of the "collective data controller" (which authority should sign and execute the agreement?). Once GDPR becomes fully applicable, most likely provisions of Polish law under which the "collective data controller" was created will stop being binding.

Anticipated changes to Polish personal data protection law

In relation to the requirements of the regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR), member states are entitled to provide specific rules in certain areas of personal data processing.

Polish Ministry of Digitalization has started working on an act on personal data protection which will provide such specific rules for Poland. The act is supposed to be voted by the Polish Parliament in autumn 2017.

Key Contacts

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

Russia

Overview

The Federal Service for Supervision of Communications, Information Technology, and Mass Media – Roskomnadzor is the Russian state regulator in charge of data protection oversight. Roskomnadzor ensures compliance of data controllers and data processors with the Russian Personal Data Law and has the authority to:

- request from individuals and legal entities information within the scope of authority;
- conduct scheduled and unscheduled audits and regular monitoring;
- request data controllers to amend, block or erase personal data which is incorrect or has been unlawfully collected;
- take measures in order to suspend or terminate data processing if it violates the Personal Data Law, including blocking of access to violator's website;
- file claims in court for the protection of data subjects' rights;
- issue compliance orders;
- request competent state authorities to initiate administrative and criminal proceedings for breach of data subjects' rights.

2016 ENFORCEMENT ACTIVITY

Russia (1 September 2015 – 29 August 2016)	
Compliance orders	2314 (1822 following the results of audits, 492 following the results of ongoing monitoring)
Websites blocked	161 (based on 59 court orders)

Most notable enforcement actions for 2016

In 2015 the total amount of fines imposed for violation of Personal Data Law was over 10,4 million RUB (approx. 165,000 EUR). At the time of this publication, the data for 2016 is yet unavailable.

The most widely discussed sanction imposed on data controllers in 2016 was blocking of access to the infringing websites. For a website to be blocked in Russia, a court order is required. Once the court decision enters into force, Roskomnadzor adds the website to the register of violators of data subjects' rights and instructs Russian telecom operators to block access to it. As a rule, this procedure does not take more than a few days.

The most prominent example of a website blocked from Russia for violation of the Personal Data Law is the LinkedIn case. Early in 2016 following the information about the LinkedIn leaks, Roskomnadzor requested the platform to confirm compliance with the data localisation requirement. After a repeated request remain unanswered, Roskomnadzor brought the case to court. In August 2016, the court of first instance found LinkedIn liable for breach of data protection rules and ordered to block access to the platform from Russia. In November 2016, the decision was upheld by the appellate court.

Several key aspects of the Russian personal data regime were discussed during the trials. Firstly, the case confirmed that foreign companies targeting Russian audience are subject to the Personal Data Law, irrespective of whether they have business presence in the country. LinkedIn met the criterion of targeting Russian market because its website was available in Russian and it allowed Russian-language advertising. Secondly, the case demonstrated that domain administrator may be liable for unlawful processing of personal data, which is collected through the website at its domain. Based on the circumstances of the case, LinkedIn Corporation was found in breach of data localisation requirement despite the fact that Russian users signed the user agreement with LinkedIn Ireland.

Shortly after the judgement of the appellate court came into force access to LinkedIn.com from Russia was blocked. No fine was imposed.

Hot topics / key developments for 2016

In 2016, enforcement of data localisation requirement remained a hot data protection topic in Russia. Since the introduction of the requirement in September 2015, the regulator's approach to its enforcement has been to engage in a dialogue with data controllers, particularly with large international companies operating in Russia. If the controllers demonstrated willingness to move processing of the data they collect in Russia to Russian servers, Roskomnadzor refrained from imposing sanctions and allowed time to come into compliance.

Summarising the data protection enforcement practice in 2016, the head of Roskomnadzor identified the LinkedIn case as a milestone of key significance for the Russian Internet. At the same time, the state official urged not to view it as a precedent for other social media platforms operating in Russia. These statements were made after LinkedIn representatives met with Roskomnadzor officials and were assured that access to the platform will be restored when it complies with data localisation requirement.

Another topic, trending in 2016 was an initiative to create a regulatory regime for anonymous unstructured data generated by Russian Internet users, which currently falls outside of personal data protection scope. At Saint Petersburg International Economic Forum held in summer of 2016, the head of Roskomnadzor proposed to establish a public-private partnership, which would act as a national big data operator facilitating data transfers and ensuring data protection. In November 2016, media reported that a working group

within the Presidential Administration was drafting a roadmap for implementation of a regulatory framework for 'big user data'. These discussions demonstrate the increased awareness of the state of the political and commercial value big data holds and are likely to result in tangible measures.

Key Contacts

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

Konstantin Bochkarev
+48 (0) 519 50 6226
anna.kobylanska@pl.pwc.com

Paulina Smykouskaya
+7 (495) 967 6000
paulina.smykouskaya@ru.pwc.com

Spain

Overview

Fines, legal opinions, international transfer authorizations, information rights enforcement

2016 ENFORCEMENT ACTIVITY

SPAIN (2016)	
Monetary Penalties (i.e. fines)	540
Information rights enforcement	1965
Legal opinions	2
International transfers authorizations	478

* These statistics are not official.

Most notable enforcement actions for 2016

Official figures and enforcement trends will not be released until midyear, most relevant fines issued taking into account the special echo in media have been:

In June, the SDPA issued a €150.000 penalty to Google. The decision proved that after the right to be forgotten requested by a user, Google notified to affected websites whose link was removed from the search results. The SDPA understood that this practice jeopardizes the complainant's right to be forgotten and considered as a serious breach of the secrecy of data.

Dissemination on the Internet of contents of a judicial summary not previously anonymised entailed to a Spanish non-profit association a € 100.000 fine. The SDPA considered the facts as a very serious and a serious infringement derived from, respectively, having released sensitive data and breaching secrecy obligations.

In September 2015, the SDPA imposed a 20,000€ penalty to Telefonica Movistar. The SDPA declared that Telefonica was using "header enrichement" at the time the consumers accessed the internet without informing them properly, nor receiving their approval in an adequate manner. resulting in a clear infringement of the article 22.2 of the Spanish law of Information Society Services and Electronic Commerce (LSSI). Such technique allowed the company to identify the consumers and, at the same time, to use the information for different economic purposes,

Hot topics / key developments for 2016

The Spanish Data Protection Office issued guidance for the re-use of public sector information aiming at ensuring full guarantees of the data subject rights.

The guidance, addressed to manager of public institutions, includes the aspects that should be taken into account to make the information available with due guarantees in terms of data protection.

Additionally, the SDPA has also published a guidance on the procedures for the anonymisation of personal data.

The SDPA released a FAQs questionnaire that gives response to the main implications in relation with the implementation of the General Data Protection Regulation.

Along with it, the SDPA subsequently released a press note analysing the main concerns of the entities (such as consent, information duties, PIA…) for the implementation of the General Data Protection Regulation by the entities.

Assumpta Zorraquino
+48 (0) 519 50 6226
anna.kobylanska@pl.pwc.com

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

Sweden

Overview

In Sweden, the Data Protection Authority (DPA) has the responsibility to enforce the Data Protection Act, the Debt Recovery Act and the Credit Information Act.

They perform inspections in two ways: by visiting an organization for inspection or by sending out a survey. The DPA has the power to issue penalties. The DPA will often provide advice on how an organization can improve its privacy policies and procedures and/or make them sign undertakings. Any decision or penalty issued by the DPA may be appealed in the Administrative Court. An inspection may be made by the DPA 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 DPA if the organization does not implement the PDR's request to rectify identified violations of the Personal Data Act. The PDR role is similar to the DPO role, but there are no formal competency requirements. It is voluntary for an organization to appoint someone. The PDR is expected to ensure that an organization complies with the Data Protection Act by providing appropriate related advice.

2016 ENFORCEMENT ACTIVITY

This is a short summary of the enforcement actions taken by the Swedish Data Protection Authority (DPA) in 2016:

Camera surveillance	7 (hotel, home care service, restaurants)
Credit information	3 (credit information companies only)
Debt recovery	24 (debt recovery companies)
Personal data	25 (social welfare, police, public authorities, telecom and internet providers, banks, finance companies)

In relation to earlier years, the amount of enforcement actions taken concerning personal data has highly decreased. In 2014 the total amount of enforcement actions was 211, in 2015 it was 103 and the past year the Swedish Data Protection Authority (DPA) has taken 59 enforcement actions on companies and authorities. This reveals that the main focus is now on preparing for the new General Data Protection Regulation. But the yearly amount of enforcement actions taken is also based on different enforcement projects taken by the DPA from year to year. Sometimes the DPA focus on a specific industry which generates a higher amount of enforcement actions. DPA is also working proactively with awareness actions, which is another reason to the decreasing amount of enforcement actions the past year.

Prosecutions

The Swedish Protection Authority aimed harsh criticism at the Stockholm police for keeping a secret database of notes about women who had called in to report that they were subjected to domestic abuse. The DPA determined that the register was illegal, a judgement which was later shared by the Administrative court.

One of the district courts sentenced a nurse to pay a fine after she unlawfully read the medical journals of a patient. The nurse was sentenced to a daily penalty payment for 40 days and a compensation of 5000 SEK to the victim. Another individual was sentenced to pay a compensation of 15000 SEK to a convicted criminal on charges of slander on Facebook and violations on the Personal Data Act.

The Supreme Administrative Court of Sweden determined that petroleum companies do not have the right to blacklist vehicles that fuel without paying. The Supreme Administrative Court considered that the purpose of blacklisting cannot motivate the intrusion into privacy that the processing is causing. Therefore, reasons to provide exemptions from the Personal Data Act were missing. This is the first time that the Supreme Administrative Court considered determination to provide exemptions from the Personal Data Act in cases of processing personal data concerning crimes.

The Supreme Administrative Court of Sweden also ruled that camera drones qualify as surveillance cameras and require permit under Sweden's camera surveillance laws. The ruling require drone owners to pay a fee to get a permit to fly. However, paying is no guarantee a drone owner will be granted the right to fly. There are no exceptions made for commercial use. The Supreme Administrative Court of Sweden also decided that dash cams and cameras affixed to bicycles are not in violation of the public's right to privacy, since the devices are within reaching distance of the people who are operating them, in opposite of camera drones. Sweden is one of the first countries to ban camera drones without special surveillance permit.

Key Contacts

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

Sofie Alberg
sofie.alberg@se.pwc.com

Switzerland

Overview

According to the Federal Act of Data Protection (FADP), the Commissioner can investigate cases of data processing in more detail, on his own initiative or the request of a third party (Art. 29). Subsequently, the Commissioner may recommend that the method of processing be changed or abandoned. If a recommendation made by the Commissioner is not complied with or is rejected, he may refer the matter to the Federal Administrative Court for a decision. He has the right to appeal against this decision and proceed to the Swiss Federal Supreme Court.

If the Commissioner establishes in a case investigation that the data subjects are threatened with a disadvantage that cannot be easily remedied, he may apply to the President of the division of the Federal Administrative Court responsible for data protection for interim measures to be taken (Art. 33).

Finally, private persons are liable to a fine if they wilfully breach obligations to provide information, to register or to cooperate (Art. 34). Fines in case of a privacy violations are currently max. 10,000 Swiss francs. Those fines are not issued by the Commissioner but by cantonal courts.

2016 ENFORCEMENT ACTIVITY

CH (2016)	
Recommendations	2
Interim measures	none

Fines

No data available as it is subject to cantonal court decisions and this data is not publicly available.

Most notable enforcement actions for 2016

The Commissioner cannot issue fines.

Hot topics / key developments for 2016

In December 2016, the Federal Council published the preliminary draft for the revision of the Swiss Federal Data Protection Act (FDPA). The revision's focus is to strengthen data protection and the individual rights of citizens. At the same time, developments at European level are taken into account, in particular the recently adopted General Data Protection regulation (GDPR) of the European Union and the Data Protection Convention of the Council of Europe (ETS 108).

Companies will be required to inform comprehensively about their data processing. Additional notification and documentation obligations are introduced. Reflecting the GDPR, privacy by design and privacy by default are new legal concepts that will be introduced. Self-regulation (good practice) is a new approach that will be fostered by the law.

The competencies of the Federal Data Protection and Information Commissioner (FDPIC) will be fundamentally strengthened. It will have the power to investigate violations independently and to issue corresponding remedial orders. Sanctions will considerably be tightened. Fines in case of privacy violations are increased from currently max. 10,000 Swiss francs to a new maximum of CHF 500,000 Swiss francs. A breach of a professional secrecy obligation will impose a threat of imprisonment.

The revision of the FDPA will have a material and significant influence on how companies will process data in the future. Henceforth, violations of the new rules can – in contrast to today – be sanctioned severely. Revision is envisaged to be completed in the summer of 2018.

Key Contacts

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

UAE

Overview

The most comprehensive data privacy law in the UAE is the Federal Decree Law No 5 of 2012 on Combating Cybercrimes (the "Cyber Crimes Law") which introduces a wide range of offences and penalties, whilst criminalizing the invasion of one's privacy and exposure of confidential information by electronic means. Besides providing for significant financial penalties and custodial sentences, and the deportation of foreigners convicted of any offence under the law, the Cyber Crimes Law empowers the authorities to seize and destroy equipment used in the commission of the offence. Financial penalties under the Cyber Crimes Law range from fines between AED 150,000 to 1,000,000. Imprisonment is also a possible sanction which may be applied against the general manager or another individual who was responsible for the breach.

The UAE Penal Code makes it a crime to publish any personal data which relate to an individual's private or family life. Infringement of an individual's privacy right is enforceable by the public prosecutor in the criminal courts and could result in a fine of up to AED 20,000 and/or imprisonment up to a year (please see above).

A number of UAE laws regulate specific sectors in the UAE through the introduction of data security elements applicable to the collection, processing, storage and use of personal data. As an example, the Telecommunications Regulatory Authority has the authority to impose an administrative fine of up to AED 10 million against licensees for violating the law or its executive order, decisions and regulations.

The Dubai International Financial Centre ("DIFC"), which has its own data protection laws and regulations, established the Office of the Data Protection Commissioner ("ODPC"). The ODPC conducts supervisory visits to DIFC organisations and has the power to issue warnings, impose fines in the event of non-compliance with its directions and with the DIFC laws, as well as initiate claims for compensation before the DIFC Courts on behalf of a data subject where there has been a material contravention of the Law.

2016 ENFORCEMENT ACTIVITY

Please note that there are extremely limited instances of reported fines or sanctions for breach of data protection and security issues in the UAE. Public policy in the UAE restricts such information being made public unless there is a particular matter of public interest which the press publicises.

Most notable enforcement actions for 2016

Please note that there are extremely limited instances of reported fines or sanctions for breach of data protection and security issues in the UAE. Public policy in the UAE restricts such information being made public unless there is a particular matter of public interest which the press publicises.

Hot topics / key developments for 2016

A new federal law, No. 12/2016, made it a punishable offence for individuals to use virtual private networks (VPNs) for the purpose of committing a crime or preventing its discovery. The offence can be punishable by temporary imprisonment (please see above) and/or a fine of no less than AED 500,000 and not exceeding AED 2,000,000.

The Abu Dhabi Global Market, the UAE's new financial free zone, recently published Data Protection Regulations that introduce specific provisions with regards to the collection, use and distribution of individual personal data. The regulations also provide for rights of 'data subjects' (such as rights to access, rectify or erase personal data), registrar-level powers to issue warnings, as well as remedies, liabilities and sanctions for contraventions.

Key Contacts

Alan Wood
+971 (0) 4 304 3739
alan.wood@pwc.com

USA

In the United States, federal agency enforcement and private litigation surrounding privacy and data security issues saw an increase in activity, with nearly $250 million in privacy and security related fines.

The Federal Trade Commission ("FTC") has the power to take law enforcement action to ensure companies live up to their promises to safeguard consumer information and to protect from unfair or deceptive trade practices, deriving authority from Section 5 of the Federal Trade Commission Act.

The Federal Communications Commission ("FCC") is becoming more active in protecting consumer privacy and security in recent years, regulating telecommunications carriers' privacy and security programs under Section 222 of the Communications Act of 1934, and the Telephone Consumer Protection Act of 1991.

The U.S. Department of Health and Human Services ("HHS") Office for Civil Rights ("OCR") is responsible for enforcing the Privacy and Security Rules. The number of OCR investigations is increasing annually. Since 2003, OCR's enforcement activities have obtained significant results that have improved the privacy practices of covered entities.

Private class action lawsuits arising out of privacy and security violations lead to a large volume of litigation involving the collection, use, or transfer of consumer information, and alleged intrusions upon privacy interests in 2016.

2016 FTC activity (over $3 million in fines)

Despite seemingly low numbers in 2016, FTC fines are nearly on par with 2015. In 2016, several organizations received initial penalties that were much higher than the final decision, due to organizations' financial situations and inability to pay the original, higher penalty. 2015 also saw the highest privacy-related fine ever recorded by the FTC, coming in at $100 million (LifeLock).

2016 FCC activity (1.35 million in fines)

The FCC focus is a relatively new entity enforcing privacy-related actions. Rollback of the FCC's new broadband privacy rules are likely to garner significant attention in 2017.

2016 HHS activity (over $20 million in fines)

The OCR focuses on the protection of health care information, and sharpened its focus in 2016, piling on heavy penalties which doubled since 2015.

2016 Class Action activity (over $223.5 million in fines)

The escalating area of privacy class action litigation, specifically Telephone Consumer Protection Act ("TCPA") litigation, showed no signs of slowing down in 2016. The TCPA restricts telephone and facsimile solicitations – such as telemarketing, junk faxes, and the use of automated telephone equipment, including automatic dialling systems, artificial or pre-recorded voice messages, and SMS text messages. It also specifies identification and contact information of the entity using the device to be contained in the message. Several TCPA related class action suits were settled this past year.

Most notable actions for 2016

Online dating site Ashley Madison failed to take basic steps to safeguard users' personal data, such as having a written information security policy and training for its employees, and was fined $17.5 million by the FTC, but was reduced to $1.6 million due to the company's "financial situation." The deal also requires the defendants to undertake a series of corrective measures, including implementing a comprehensive data-security program and having their practices assessed by a "qualified, objective, independent third-party professional" every two years."

Verizon Wireless was fined $1.35 million by the FCC for implementing "supercookies"—unique, undeletable identifiers ("UIDH")—in 2012 to track customers' online behavior, but did not disclose this information to customers, amend their privacy policies to reflect this, or offer an opt-out for over two years.

HHS settled with Advocate Health Care, one of Illinois' largest hospital chains, for $5.5 million for a series of data breaches involving the unprotected and sensitive healthcare information of over 4 million patients at a medical group subsidiary due to the enforcement of appropriate security and privacy controls.

Caribbean Cruise Lines settled a TCPA class action lawsuit for up to $76 million, but not less than $56 million, for robocalling millions of individuals with offers for free trips without first seeking consent.

Hot topics / key developments for 2016

With President Trump entering the White House, there could be a "true paradigm shift" in the way the U.S. treats cyberattacks and hacking attempts on government agencies and U.S.-headquartered companies. The new administration could build on the work of President Obama in pushing the operators of critical infrastructure and U.S.-headquartered multinationals to address cybersecurity weaknesses. Over the last 10 years, the U.S. has not retaliated to significant cyberattacks by foreign states, despite knowing where the hacks originated. If the U.S. changes tactics, one consequence could be the first catastrophic attack on critical online infrastructure – such as an attack with a wide-reaching impact on business or a shutdown of financial systems, power grid or transportation system.

Anticipated changes to United States privacy law

Privacy regulation in 2017 is in a current state of uncertainty, as the new presidential administration determines their stance on issues – such as unifying state breach notification laws, government access to personal data, and the relationship between service providers and law enforcement. Furthermore, FCC regulations adopted in October 2016 during the Obama-era requiring internet service providers to do more to protect

consumer privacy – such as obtain consent before using geolocation and other personal information -- were overturned in March 2017, leaving U.S. privacy law in a state of flux. General Data Protection Regulation ("GDPR") implementation, the IoT, and "smart toys" are all issues that will garner attention in 2017.

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

Daniel Pomierski
+1 (312) 298-5583
daniel.pomierski@pwc.com

Team and Contact Information

Strategy, Compliance and Legal Services team

Stewart Room
Partner
+44 (0)20 7213 4306
stewart.room@.pwc.com

James Drury-Smith
Director
+44 (0)20 7212 1599
james.drury-smith@pwc.com

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

Kate Macmillan
Director
+44 (0)20 7213 4306
kate.macmillan@pwc.com

Polly Ralph
Senior Manager
+44 (0)20 7804 1611
polly.ralph@.pwc.com

David Cook
Manager
+44 (0)161 245 2485
d.cook@.pwc.com

Jane Foord-Kelcey
Manager
+44 (0)7525 897 862
jane.foord.kelcey@pwc.com

James De Cort
Manager
+44 (0)7710 035 635
james.de.cort@pwc.com

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

Samantha Sayers
Senior Associate
+44 (0)7841 803 730
samantha.sayers@pwc.com

Kayleigh Clark
Senior Associate
+44 (0)7701 297 345
clark.kayleigh@pwc.com

Fiona Bundy-Clarke
Senior Associate
+44 (0)7841 468 725
fiona.bundy-clarke@pwc.com

Natasha Simmons
Senior Associate
+44 (0)7841 803 730
natasha.simmons@pwc.com

Tughan Thuraisingam
Senior Associate
+44 (0) 207 804 3770
tughan.thuraisingam@.pwc.com

Lewis Brady
Senior Associate
+44 (0) 207 804 3770
lewis.w.brady@pwc.com

Jamie Witton
Senior Associate
+44 (0) 207 804 2509
james.witton@pwc.com

Olivia Wint
Senior Associate
+44 (0) 7710 035 127
olivia.wint@pwc.com

Yaw Kusi
Senior Associate
+44 (0) 7808 799 885
yaw.kusi@pwc.com

Sara Jameel
Associate
+44 (0) 7718 978 175
sara.e.jameel@pwc.com

Rima Karia
Associate
+44 (0) 7841 468 299
rima.karia@pwc.com

Shervin Nahid
Associate
+44 (0) 7841 468 308
shervin.nahid@pwc.com

Lucy Tucker
Associate
+44 (0) 207 212 2299
lucy.c.tucker@pwc.com

Tamsin Hoque
Associate
+44 (0) 207213 1783
tamsin.hoque@pwc.com

[PwC] 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

Jonathan Turner
Partner
+44 (0) 207 213 5565
jonathan.v.turner@pwc.com

Rav Hayer
Partner
+44 (0) 207 213 3415
rav.hayer@pwc.com

Michael Campbell
Partner
+44 (0) 7702 678 053
michael.campbell@pwc.com

Andrew Cameron
Partner
+44 (0) 7841 467 226
andrew.cameron@pwc.com

Raoul Rambaut
Partner
+44 (0) 7801 216 660
raoul.c.rambaut@pwc.com

Christopher Reeve
Partner
+44(0)20 780 47568
chris.a.reeve@pwc.com

Jonathan Boulton
Partner
+44 (0)113 288 2080
jonathan.m.boulton@pwc.com

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

Tayyaba Arif
Director
+44(0)20 780 46148
tayyaba.arif@pwc.com

Peter Almond
Director
+44 (0) 7793 758 029
peter.almond@pwc.com

Michael Orr
Partner
+44(0)28 9041 5363
michael.g.orr@pwc.com

Shabdeep Mann
Director
+44(0)20 780 44835
shabdeep.mann@pwc.com

Craig Mckeown
Director
+44(0)28 9041 5068
craig.l.mckeown@pwc.com

Asam Malik
Director
+44(0)191 269 3332
asam.malik@pwc.com

James Rashleigh
Director
+44(0) 20 7212 2060
james.m.rashleigh@pwc.com

Chris Neil
Senior Manager
+44 (0) 7738 844 762
chris.r.neil@pwc.com

Rahul Colaco
Senior Manager
+44 (0) 7702 677 404
rahul.p.colaco@pwc.com

Gareth Neal
Senior Manager
+44(0)161 245 2274
gareth.p.neal@pwc.com

Rachel Washington
Senior Manager
+44 (0) 77150 33722
rachel.washington@pwc.com

Maria Roman
Senior Manager
+44 020 7213 1187
maria.roman@pwc.com

Corina Scott
Manager
(646) 471-4587
corina.scott@us.pwc.com

Stuart Harvey
Senior Manager
+44(0)20 780 42485
stuart.j.harvey@pwc.com

Ciaron Nelis
Senior Manager
+44 (0)7739 196 813
ciaron.nelis@pwc.com

Denzil Coelho
Senior Manager
+44 (0) 7725 706 596
denzil.a.coelho@pwc.com

Angelica Pena
Manager
+44(0)20 7804 3220
angelica.pena@pwc.com

Sail Wadhwani
Manager
+44(0) 20 7213 4977
sail.wadhwani@pwc.com

Andrew J Powell
Manager
+44 (0)161 245 2380
andrew.powell@pwc.com

Lola Ladejobi
Manager
+44 (0) 7889 155 245
lola.m.ladejobi@pwc.com

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

Edward Starkie
Senior Associate
+44 (0)207 213 5074
edward.starkie@pwc.com

Joseph Corina
Senior Associate
+44 (0)770 269 9188
joseph.corina@pwc.com

Rayyan Aleem
Senior Associate
+44(0)20 780 44353
rayyan.a.aleem@pwc.com

Andrew Pope
Senior Associate
+44(0)20 780 43283
andrew.j.pope@pwc.com

Christopher Williams
Senior Associate
christopher.x.williams@pwc.com

International Lawyers

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

Sylvia Ng
Australia
+61 (2) 8266 0338
sylvia.ng@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

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

Sandrine Cullaffroz-Jover
France
+33 (15) 65 74 029
sandrine.cullaffroz-jover@pwcavocats.com

Pauline Darnand
France
+33 (38) 84 53 261
pauline.darnand@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

Flavia Messina
Italy
+39 (02) 916 05 054
flavia.messina@it.pwc.com

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

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

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

Paulina Smykouskaya
Russia
+7 (495) 967 6000
paulina.smykouskaya@ru.pwc.com

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

Konstantin Bochkarev
Russia
+48 (0) 519 50 6226
anna.kobylanska@pl.pwc.com

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

Alan Wood
UAE
+971 (0) 4 304 3739
alan.wood@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

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

Maria Koslunova
Canada
+1 (416) 941 8383
maria.koslunova@ca.pwc.com

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

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

Faiz Haque
India
+91 8130064263
faiz.haque@in.pwc.com

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

Lars Erik Fjørtoft
Norway
+47 (0) 974 74 469
Lars. Fjørtoft@pwc.com

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

Sofie Alberg
Sweden
sofie.alberg@se.pwc.com

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

Daniel Pomierski
USA
+1 (312) 298-5583
daniel.pomierski@pwc.com

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

www.pwc.co.uk