GLOBAL PRIVACY ENFORCEMENT REPORT 2015

DataGuidance | Research

DATAGUIDANCE

DataGuidance is the leading global privacy compliance service, designed to make it easier, faster, and more cost effective to maintain control of your worldwide privacy programme.

DataGuidance 17 The Timber Yard, Drysdale Street, London, UK **T** 0207 012 1380 **E** david.longford@dataguidance.com www.dataguidance.com

FOREWORD AND METHODOLOGY

GLOBAL ENFORCEMENT

Welcome to this year's Enforcement Report, prepared by DataGuidance's team of Privacy Analysts in collaboration with their network of legal experts. DataGuidance understands the value in staying abreast of enforcement action taken by national Data Protection Authorities (DPAs) and the potential risks associated in operating in particular jurisdictions as a result of the same. Building on our previous two Reports, DataGuidance has expanded its coverage to include a truly global breakdown of the enforcement action taken by national regulators during 2014 in Europe, Asia Pacific, Latin America, North America and the Commonwealth of Independent States (CIS).

As each jurisdiction is unique in terms of legislation and the powers that are afforded to the regulator responsible for privacy compliance, this year's Report includes detailed insight from leading privacy lawyers, selected for their specialised knowledge of the enforcement regimes in place. In addition, it provides analysis into significant DPA decisions and case law, in an effort to unearth the practical reality of privacy risk at a local level.

The Report highlights that 2014 was yet another busy year for the regulators in terms of both penalties issued and the changing nature of their powers. In France, Google received a $181,650 fine for changes to its privacy policy implemented in March 2012, whilst in Australia and the Netherlands, amendments to legislation provide greater powers to the Office of the Australian Information Commissioner and Dutch Data Protection Authority to impose monetary penalties against organisations for breach of data protection laws.

Whilst the Report highlights a point in time, DataGuidance continually monitors enforcement as part of its Daily Updates service, in order to keep you and your privacy team at the forefront of the latest developments throughout the year. DataGuidance also plans to incorporate the data collected in this Report to form an interactive tool available on its platform.

METHODOLOGY

To compile the information in this Report, DataGuidance's Privacy Analysts made extensive use of the Annual Reports issued by DPAs, as well as liaising with their network of Contributors. DataGuidance posed questions to both regulators and Contributors, requesting breakdowns of action taken in respect of penalties issued, as well as notable decisions and judgments from each jurisdiction listed. DataGuidance also requested information relating to the maximum potential penalties and custodial sentences that can be imposed for breaches of data protection legislation. DataGuidance focused on enforcement action brought by national DPAs, however, in certain jurisdictions where no DPA is present, DataGuidance sought information from its Contributors in relation to the wider privacy enforcement landscape.

All amounts have been converted to Dollars at the exchange rate set on 31 December 2014.

TABLE OF CONTENTS

EUROPE

Austria

The Austrian Data Protection Authority **does not have the power** to issue fines.

Maximum potential penalty: $30,275 (to be issued by the competent District Administrative Authority).
Maximum potential custodial sentence: 1 year (to be issued by the Courts under specific circumstances).

Dietmar Huemer, Partner at Legis

Belgium

The Belgian Commission for the Protection of Privacy (CPP) **does not have the power** to issue fines.

Maximum potential penalty: $726,000 (criminal penalty to be decided by judicial courts)
Maximum potential custodial sentence: 2 years (under specific circumstances)

“ The CPP has initiated a lawsuit against Facebook regarding its new terms of use which entered into force on 30 January 2015. The CPP considers, amongst others, that these terms of use enable Facebook to track both users and non-users without obtaining proper consent from the latter. The action is currently pending in summary proceedings in Brussels ”

Tanguy Van Overstraeten and Clément Legrand, Partner and Associate at Linklaters LLP

Bosnia & Herzegovina

No. of penalties	Total amount	Average
12	$8,036	$670

Biggest penalty $6,055

Maximum potential penalty $60,550

Selma Šehović, Senior Associate at Marić & Co. LLC

Croatia

The Croatian Data Protection Authority **does not have the power** to issue fines, however, fines may be issued by courts.

Maximum potential penalty: $6,418
Maximum potential custodial sentence: 5 years

***Note:** The below figures relate to 2013 enforcement

“ The AZOP’s report provides that it: (i) submitted 2 cases to the courts for violations of data privacy laws under the Croatian Data Protection Act 2003; and (ii) submitted 4 cases to the State Attorney and Police for suspicion on possible criminal offenses related to data privacy ”

Marija Gregorić, Partner at Babić & Partners

Cyprus

No. of penalties	Total amount	Average
8	$11,141	$1,393

Biggest penalty $3,633

Maximum potential penalty $36,330

Maximum potential court penalty: $6,206

Maximum potential custodial sentence: 3 years

Nicholas Ktenas, Partner at Andreas Neocleous & Co LLC

Czech Republic

No. of penalties	Total amount	Average
108	$63,685	$590

Biggest penalty $20,926

Maximum potential penalty $435,960

Maximum potential custodial sentence: 8 years

“ The biggest fine was unusually high and was issued in relation to unsolicited marketing communications. The same company was issued another penalty of $65,394 in 2015, which fell outside of the scope of the 2014 enforcement. A penalty of $12,671 was also issued to a press company for publishing records from intercepted telephone communication between the prime minister and his lover (originally recorded by police during criminal investigation) in violation of the Criminal Code ”

Richard Otevřel and Petra Sochorová, Senior Associate and Counsel at Havel, Holásek & Partners

---

Denmark

No. of penalties	Total amount	Average
5	$3,815	$763

Biggest penalty $811

No maximum potential penalty

Maximum potential custodial sentence: 4 months

Michael Hopp, Christian Wiese Svanberg and Christian Nielsen, Partner, Attorney and Paralegal at Plesner

---

Estonia

No. of penalties	Total amount	Average
8	$1,562	$195

Biggest penalty $727

Maximum potential administrative penalties: $11,626

Maximum potential fine: $1,453 for natural persons and $38,752 for legal persons

Maximum potential penalty for pecuniary punishment: For data protection violations qualifying as a criminal offence: 500 times the average daily income for natural persons and $19,367,000 for legal persons

Maximum potential custodial sentence: 1 year

Pirkko-Liis Harkmaa and Martin-Kaspac Sild, Partner and Associate at COBALT Legal

Finland

The Finnish Data Protection Ombudsman **does not have the power** to issue penalties. Criminal fines are issued as day fines, which are dependent on income of person fined. Corporate fines may not be issued for data protection offences.

Maximum potential custodial sentence: 1 year

“ In a Helsinki Court of Appeals judgement, 14/152412 Matter R 14/218 (final), ‘K’ had possessed medical records which belonged to his/her former employer as the controller, and K had had no right to process said records. The records included data on injection treatments conducted on customers of the employer. The Court of Appeal held that unauthorised processing violated the patients’ right to privacy. The Court found K guilty and sentenced K to a fine of 40 day fines ”

Eija Warma,Counsel at Castrén & Snellman Attorneys Ltd

France

No. of penalties	Total amount	Average
8 (plus 7 warnings and 3 acquittals)	$225,247	$28,156

Biggest penalty $181,650

Maximum potential penalty: In case of a first breach, the penalty may not exceed $181,650. In the event of a second breach within five years, it may go up to $363,300 or, in case of a legal entity, to 5% of gross turnover for the last financial year, with a maximum of $363,300.
Maximum potential criminal penalty: $363,300. A provision under the Commercial Code allows courts to multiply a sanction up to five times against a legal entity. In theory, a criminal court could pronounce a fine up to $1,816,500.
Maximum potential custodial sentence: 5 years

Notable decision:

“ A $181,650 fine was issued against Google Inc. for lack of information, absence of definition of a conservation period, lack of legal grounds to combine data, and lack of procedure for obtaining the person’s consent. Note that Google appealed the decision before the Conseil d’Etat (French Council of State) and then withdrew its appeal. Thus, the decision is final ”

Olivier Proust, Of Counsel at Fieldfisher
Florence Chafiol-Chaumont, Partner at August & Debouzy

Germany

State	No. of penalties	Total amount
Bavaria	20 fine notices	$242,200 (2013 & 2014 combined)
Berlin	25 fine notices	$106,816
Hesse	2 fine notices	$4,239

The **maximum potential administrative penalty** by data protection authorities in Germany is $363,300, and the maximum potential custodial criminal sentence is 2 years. In 2013/14 the **biggest fines** issued in **Bremen** and in **Schleswig-Holstein** were $18,165, and $21,798 respectively.

“ In January 2015, data protection authorities of Berlin and Bremen initiated proceedings against US companies on Safe Harbor based data transfers. This is the first time that German data protection authorities have taken legal actions based on the Safe Harbor framework. Other German authorities (e.g. Bavaria) do not share the same views and continue to permit data transfers based on Safe Harbor as long as there is no obvious breach of law ”

Andreas Splittgerber, Partner at Olswang

Greece

No. of penalties	Total amount	Average
21	$442,015	$21,047

Biggest penalty $121,100

Maximum potential penalty $177,717

Maximum potential custodial sentence: Imprisonment of up to 20 years, in the event that a criminal offence related to data protection breaches has jeopardised the free operation of democratic governance or national security.

Notable decisions:

“ Decision no. 100/2014: a company was fined $121,100 for unlawful processing of data, including sensitive data, and unsolicited communication for marketing purposes. The company possessed files of data collected illegally, without data subjects' consent, for the purpose of data trading, and was found combining data from several, both publicly available and illegally accessed, sources in order to provide its clients with customised lists of data, based on certain criteria such as income, profession or residence. In addition, the company was using e-mail addresses without recipients' consent for marketing purposes. The Data Protection Authority also sanctioned 14 other entities some of which had collaborated with the above company, and imposed fines amounting totally to $85,981 ”

Maria Giannakaki, Attorney at Law, Karageorgiou & Associates

Guernsey

“ Under the Data Protection (Bailiwick of Guernsey) Law, 2001 as amended, a person guilty of an offence under any provision of the Law other than under Section 55 (in relation to the unlawful obtaining of personal data) and Section 11 of Schedule 8 (intentionally obstructing or failing to provide assistance to a person in the execution of a warrant issued) is liable on summary conviction to a fine not exceeding level 5 on the uniform scale (currently $15,586) or on conviction on indictment to an unlimited fine.

An offence under Section 55 is liable on summary conviction, to imprisonment for a term not exceeding 12 months, or to a fine not exceeding level 5 on the uniform scale, or to both, or on conviction on indictment, to imprisonment for a term not exceeding two years, or to a fine, or to both. Under Section 11 of Schedule 8 is liable on summary conviction to a fine not exceeding level 5 on the uniform scale ”

Mark Dunster and Chloe Whitmore, Partner and Associate at Carey Olsen

---

Hungary

No. of fines issued	Total amount	Average fine
16	$317,888	$19,860

Biggest penalty $40,690

“ The Hungarian Data Protection Authority (NAIH) imposed a fine of $3,028 on a direct marketing (‘DM’) company, ordered it to revise its policies, and seek new privacy consent from its users. The company’s website enabled people to send fortune telling, virtual blessings and horoscopes to their friends in return for their consent to receiving DM messages. The NAIH launched an investigation after a complaint from a user who unsubscribed from the DM letters but kept on receiving advertisements. The NAIH launched a full-scale audit and inspected policies and operations, which the complaint did not concern. The NAIH found that the company’s external privacy policy did not specify data transfers, did not identify all data processors, did not detail data processing purposes and the rights and remedies. The NAIH also commented that it is an unlawful practice that the checkbox to the consent of the data processing is already filled in as the consent is not free this way. The NAIH also criticised that the company did not provide possibility to the relevant persons to consent separately to different data transfers - which is a new approach. It is also a novelty that the NAIH advised the company to seek a new consent from the existing users, as well as the revision of the privacy policy. The NAIH also emphasised that such revision in the course of the investigation would be considered as a mitigating factor. When determining the fine, the NAIH considered the position of the company in the market and the income indicated in its annual financial statements, which also goes beyond the criteria set out in the law ”

Márton Domokos, Senior Associate at CMS Cameron McKenna LLP

Iceland

The Icelandic Data Protection Authority (Persónuvernd) **does not have the power** to issue penalties when a breach has occurred. It can, however, impose daily fines where its instructions are not observed. In addition, penalties for a breach can be imposed by a judge in court proceedings, although no penalties were imposed by a judge in 2014.

Maximum potential penalty: According to national legislation there is no maximum amount of potential penalty that can be enforced but according to Article 51 of the Penal Code (No. 19/1940) the amount of a fine should be decided with regard of the offender's income and property, earnings, support obligations and other factors affecting his/her ability to pay and the financial gain or savings resulting from the offence or aimed at by its commission.
Maximum potential custodial sentence: 3 years

Ingvi Snær Einarsson, Attorney at Law at Lex

Ireland

"The Irish Data Protection Commissioner (DPC) **does not have the power** to issue penalties for breaches of the Data Protection Acts 1988 & 2003 (DPAs), however, the DPC can prosecute organisations for offences under the DPAs and e-Privacy Regulations 2011 (S.I. No. 336/2011). 960 complaints were received in 2014, only 27 of which required a formal decision. The remainder of complaints received were resolved amicably. The DPC prosecuted 9 entities, and served 3 enforcement notices and 9 information notices. Under the DPAs, the maximum penalty on conviction on indictment is $121,100. Under the e-Privacy Regulations, each unsolicited direct marketing call or message can attract a fine of up to $6,055 on summary conviction. If convicted on indictment, the fines range from $60,550 for a natural person to $302,750 if the offender is a body corporate"

John Whelan and Davinia Brennan, Partner and Associate at A&L Goodbody

---

Isle of Man

No cases have been taken to the Data Protection Tribunal or court. There is currently no ability to levy any monetary penalty, nor any custodial sentence available to the courts.

Data Protection Supervisor

Italy

No. of penalties	Total amount	Average
202	$2,365,083	$11,708

Biggest penalty $121,100

Maximum potential penalty: The maximum potential penalty could rise up to $2,422,000 depending on the circumstances of the case e.g. the seriousness of the violation, the annual turnover of the company etc.
Maximum potential custodial sentence: 3 years

Rocco Panetta, Partner at NCTM Studio Legale
Nadia Arnaboldi, Founder at Arnaboldi Corporate Firm
Garante per la protezione dei dati personali

Latvia

No. of penalties	Total amount
24 fines and 16 warnings	$36,754

Biggest penalty $3,445

Maximum potential penalty $87,192

Maximum potential custodial sentence: 5 years

Ilze Bulkadere, Associate at Borenius

Lithuania

No. of penalties	Total amount	Average
50	$4,505	$91

Maximum potential penalty $701

Maximum potential custodial sentence: Custodial sentences are almost never imposed in relation to data processing activities. Theoretically, an imprisonment for a term of up to 3 years can be imposed for extraordinary intrusions into one's privacy.

"The Lithuanian State Data Protection Inspectorate issued an opinion that randomly generated telephone numbers are considered to be personal data and processing of such numbers for the purpose of direct marketing without prior consent of a data subject for this reason is illegal and subject to administrative liability"

Julius Zaleskis, Senior Associate at Valiunas Ellex

Luxembourg

In Luxembourg, the National Commission for Data Protection (CNPD) **does not have the power** to issue fines, however, it is competent to issue a fine which cannot exceed $60,550 when faced with repeated infringement to the notification requirement of a breach of security.

Maximum potential court fine $151,375

Maximum potential custodial sentence: 1 year. Both sanctions are potentially cumulative

Emmanuelle Ragot and Xavier Picquet Partner and Junior Associate at Wildgen

Malta

Maximum potential custodial sentence: 6 months

Maximum potential court fine $28,216

"Decisions are not made publicly available, however, in the near future, it is the intention of the Office of the Information and Data Protection Commissioner to start publishing summaries of data protection authority decisions"

Andrew Cauchi and Dr. Yanica Borg, Director of ICT Services and Lawyer at EMD (Malta)

The Netherlands

Maximum administrative penalty: $5,450 for infringement of the general notification duty. Amendments to the Dutch Data Protection Act, entering into force on 1 January 2016, include a penalty up to $980,910, or for legal entities, 10% of the net annual turnover from the previous year per infringement of obligations under the Act. Penalties may be levied for non-compliance with the new data breach notification duties, but no longer for violation of the general notification duty. Under the Telecommunications Act, fines of up to $544,950 per infringement can be imposed by the Authority For Consumer and Markets. After 1 January 2016, some relevant enforcement powers will be transferred to the Dutch Data Protection Authority.
Maximum potential criminal penalty: $9,809 or, if the violation is intentional, then a fine of $24,523 or prison sentence of six months can be imposed (the sanction only applies for infringement of the general notification duty). These sanctions have never been imposed, and after 1 January 2016, these sanctions will not apply anymore.

"The Dutch Data Protection Authority (CBP) conducted 85 investigations in 2014 and started 13 administrative proceedings to impose an order subject to a penalty for non-compliance, but they did not lead to actual penalties. On 14 December 2014, the CBP started administrative proceedings against Google to force them to obtain unambiguous consent from data subjects for using their data across the Google services. The CBP threatened to impose an order subject to a penalty for non-compliance up to $18,165,000. Google has since taken measures to comply with the CBP's request and the DPA has indicated that it will continue to monitor Google for compliance with the Data Protection Act"

Elisabeth Thole and Eva de Vries, Of Counsel and Attorney at Van Doorne
Jeroen Lub and Kevin Van 't Klooster, Partner and Associate at Osborne Clarke

Norway

Maximum administrative penalty: Under current Norwegian legislation, the maximum penalty possible is 10 times the basis amount used in the calculation of public benefits, meaning that the current maximum is $145,956.
Maximum potential custodial penalty: Certain willful or grossly negligent breaches of the Personal Data Act 2000 are punishable with prison time of up to one year.

"There is no summary of the penalties issued by the Norwegian Data Protection Authority (Datatilsynet), however two penalties were issued in 2014, both of $10,036, plus a penalty of $80,289 which was later annulled by the Privacy Board.

In a notable case from 2013/2014, the Datatilsynet issued two penalties, each in the amount of $80,289, to Gjensidige Forsikring (a large insurance company). The first penalty of $80,289 was issued in 2013 for lack of internal control routines. The Datatilsynet then issued a second penalty of $80,289 in 2014 for illegal processing of personal data (both cases concerned Gjensidige's use of personal data from hidden investigation in insurance fraud cases concerning disability insurance claims). Gjensidige appealed the second decision, and the Privacy Board ruled that Gjensidige's processing was lawful and that the 2nd penalty of $80,289 should therefore be annulled.

The Datatilsynet has issued several penalties in 2015, resulting from inspections carried out in 2014; 5 such cases so far in 2015, including 3 penalties issued to local municipalities for lack of internal controls and one to the Department of Justice"

Øystein Flagstad, Partner at Advokatfirmaet Grette DA

Poland

No. of penalties	Total amount	Average
2	$15,743	$7,872

Note: The above figures relate to 2013 enforcement

Maximum penalty for non-compliance with an order from the Inspector General for Personal Data Protection (GIODO): $15,138. The fine may be imposed repetitively but the cumulative amount of fines cannot exceed $60,550.
Maximum potential custodial sentence: Maximum sentence is up to 12 months of limitation of freedom, or 3 years of imprisonment and/or fine of up to $326,970. But those are rather theoretical sentences. The police tend to discontinue data protection matters due to low social harmfulness.

Emilia Stępień, Founder at Law For Commerce Emilia Stępień Kancelaria Prawnicza

Portugal

The Portuguese Data Protection Authority (CNPD) has not issued its 2014 report yet. From the last available report (2012), 169 penalties were issued; the average amount of fines issued was $2,059, whilst the total amount was $342,713.

Maximum potential penalty: Up to $36,330. However, the amount may increase up to $6,055,000, for breach of the processing of personal data and the protection of privacy in electronic communications. Within the protection of privacy in electronic communications, the CNPD can impose periodic penalty payments should enforcement notices be ignored. The amount is fixed for each day, up to a maximum of 30 days and a total amount of $3,633,000.
Maximum potential custodial sentence: Up to 2 years or a penalty up to 240 days, being the amount per day established by the Court (for intentional processing in breach of the law). Undue access, invalidation or destruction of personal data, failure to comply with an order to interrupt, cease or block the processing, and violation of the duty of secrecy also constitute criminal offences under the law. In case of serious damage resulting from invalidation or destruction of personal data, it can be up to 4 years or a penalty up to 480 days, being the amount per day established by the Court.

Notable decision:

"In January 2014 the CNPD imposed a fine of $5.5 million on a mobile telecommunications operator (the highest fine known to have been applied by the CNPD) for breach of several obligations concerning the protection of privacy in electronic communications and security measures. The mobile operator appealed, however the judicial decision is not yet known"

Mónica Oliveira Costa, Partner at Coelho Ribeiro e Associados

Serbia

No. of penalties	Total amount	Average
22	$7,218	$327

Maximum potential penalty $10,051

The Serbian Commissioner for Information of Public Importance and Personal Data Protection (Poverenik) **does not have the power** to issue fines; it must apply to the court to initiate the misdemeanour proceedings.

Maximum custodial sentence: 1 year in cases of disclosure or use against the original purpose for which personal data has been collected, processed, and/or used on the basis of law and in cases of collection and use of personal data against the law. A sentence of up to 3 years can be enforced in the above cases while performing a public service.

“ Data processing by banks and other legal entities, without previously obtained consent or legal basis, has been considered as the most common irregularity in implementation of data protection regulations in 2014. However, due to the efforts of the Poverenik, most breaches of relevant provisions were rectified based on the orders of the Poverenik with no further court proceedings which gradually led to an increase of awareness of data controllers about the importance of compliance with provisions on personal data protection ”

Uroš Popović, Partner at Bojović & Partners

Spain

No. of penalties	Total amount	Average fine
776	$20,590,175	$26,534

Biggest penalty $121,100

Maximum potential penalty $726,600

Maximum custodial sentence: 7 years

Notable case law:

“ The Audiencia Nacional (Spanish High Court) sought a preliminary ruling from the Court of Justice of the European Union, which result in its landmark judgment *Google Spain SL, Google Inc v. AEPD* (C-131/12), Mario Costeja establishing the ‘right to be forgotten’ requiring the search engine delete links from search results. In addition, the Spanish Supreme Court Sentence of 3 October 2014 established that IP addresses are considered ‘personal data,’ so record companies shall not be allowed to collect information on users of peer-to-peer file-sharing networks (i.e. their IP address) without their express permission, implying that the user’s right to privacy has prevailed ”

Laura Vivet, Partner at Conditio Iuris SLP

Sweden

The Swedish Data Protection Authority (Datainspektionen) did not impose any penalties nor were there any court sentences resulting in fines, imprisonment or damages during 2014. The Chancellor of Justice did, however, grant a claimant damages of $642 for being subject to unlawful data processing. The majority of measures taken during 2014 constitute remarks and injunctions issued by the Datainspektionen.

Maximum potential penalty: There is no fixed limit to the amount that a conditional fine may be set, beyond that it must be proportional to the importance of the objective of the order. Under the Data Protection Act 1998 and the Swedish Penal Code they consist of fine units ranging between 30 and 150 units. The monetary amount of a fine unit is assessed depending on the convicted persons financial situation, and may be set within the interval of $6 to $128.

Henrik Nilsson and Sandra Lima, Partner and Associate at Gärde Wesslau Advokatbyrå

Switzerland

Maximum potential penalty $11,505

The Swiss Federal Data Protection and Information Commissioner **does not have the power** to issue penalties for infringements of the Swiss Federal Data Protection Act 1992. No judgments on such penalties have been published. However, according to the Swiss Federal Statistical Office, 7 infringements of Article 34 and/or 35 of the Act have been reported in 2014. However, there are no statistics available on the amount of the penalties issued and as the statistics are incomplete, the actual number of penalties issued in 2014 is most likely higher.

Maximum potential custodial sentence: 3 months under Articles 34 and 35 of the Act in connection with Article 106 Para. 1 of the Swiss Penal Code; however, note that a custodial sentence will only be enforced if a fine is wilfully not paid. Please note, the maximum custodial sentence pursuant to Article 179novies of the Swiss Penal Code, is 3 years.

Jürg Schneider, Dr. iur., Attorney at Law and Partner at Walder Wyss Ltd

---

United Kingdom

No. of penalties	Total amount	Average
11	$1,796,238	$163,294

Biggest penalty $311,711

Maximum potential penalty $779,279

During the UK Information Commissioner's Office (ICO) press conference for its 2014 annual report, Deputy Commissioner David Smith noted that the ICO issued 11 civil monetary penalties (CMP), totalling $1,796,238, and $601,603 of which related to unsolicited marketing calls and texts. The figures show a decrease in the amount of CMPs issued, as the ICO issued a total of $3,070,357 in 2013. Despite this, Smith pointed out that the ICO had increased its enforcement of the private sector. 'We have come down firmly on those not adopting best security practices, but not necessarily those that have suffered a security incident,' he stated.

Hazel Grant, Antonis Patrikios and Samantha Sayers, Partners and Solicitor at Fieldfisher

ASIA PACIFIC

Australia

Maximum potential penalty $1,388,146

“ The ability to seek to impose ‘penalties’ for breaches of the privacy principles only entered into Australian privacy law from 12 March 2014 with the introduction of the changes to the Privacy Act 1988 and the new Australian Privacy Principles (APPs). Before 12 March 2014 the usual outcome of investigations/enforcement actions were the awarding of ‘remedies’ by the Privacy Commissioner (which is still a preference of the Privacy Commissioner post 12 March 2014). ‘Remedies’ include apologies, access to the information, requiring staff training, changed procedures and/or corrections of the information and also include compensation in the amount determined by the Privacy Commissioner. In 2014 remedies were awarded by the Privacy Commissioner in a total of 439 cases, with **compensation awarded in 49 of those cases**. The largest amount of compensation awarded by the Privacy Commissioner was $14,724 ”

Maximum potential penalty: Since 12 March 2014, the maximum penalty that can be sought by the Privacy Commissioner to be imposed is $1,388,146 for entities (i.e. private organisations and Federal Government agencies) and $292,844 for individuals for serious or repeated breaches of the APPs.
Maximum potential custodial sentence: Failure/refusal to attend before the Privacy Commissioner, when requested, and/or failure or refusal to give the information requested by the Privacy Commissioner (e.g. answer questions, produce a documents etc) may attract a penalty of up to12 months' imprisonment on conviction.

Alec Christie, IP/IT Data Privacy Law Partner at EY

China

“ In addition to the courts, two government agencies have the authority to issue penalties for personal data infringement. Firstly, the local ministries for information industry (‘local MIIs’) have the authority to impose penalties on telecoms and Internet business operators located in their respective jurisdictions for violations of the Telecoms and Internet User Information Protection Regulation (the ‘Information Regulation’). Secondly, the local administrations for industry and commerce (‘local AICs’) have the authority to impose penalties on all business operators located in their respective jurisdictions for violation of the Consumer Interest Protection Law (‘Consumer Protection Law’) ”

Maximum potential penalty: For violations of the personal data protection requirements under the Information Regulation regarding the use and collection of personal data (by itself or through third parties); protection against data leakage; internal training; and self-inspection of the business’s protection measures, local MIIs have the authority to impose orders to make corrections, warnings and fines up to $4,833.

Under Article 56 of the Consumer Protection Law, a violation of personal data protection requirements may result in an administrative order for rectification. Where the violation has resulted in illegal gains, local AICs have the authority to impose fines up to 10 times of the gains. Where no illegal gains were involved, the maximum fine is $80,500. In serious circumstances, offenders may be ordered to suspend their business for rectification and have their business licenses revoked.

Alex Shepherd, Carolyn Bigg, Yang Xun and Aaron Patience, Partner, Managing Associate, Counsel and Managing Associate at Simmons & Simmons with the assistance of, and advice from, **JWS Asia Law Corporation and TMI Associates**

Hong Kong

Maximum potential penalty: $128,900 for the unauthorised transfer of personal data to third parties for direct marketing purposes or for sale.
Maximum potential custodial sentence: Five years' imprisonment for the unauthorised transfer of personal data to third parties for direct marketing purposes or for sale.

The Office of the Privacy Commissioner for Personal Data (PCPD) issued **20 warnings** and **90 enforcement notices** in 2014. In 2014, the PCPD also referred **20 cases to the police**, resulting in **one conviction**.

Notable decisions:

" In 2014, the PCPD took a number of enforcement actions relating to the unnecessary and unjustified collection of data, following PCPD investigation. In particular:
(i) In November 2014, the PCPD served enforcement notices on five companies/proprietors running tutorial service agency websites, requiring them to stop unnecessarily collecting personal data of private tutors, including identity card numbers.
(ii) In November 2014, the PCPD served enforcement notices on 10 employment agencies for domestic helpers, directing them to cease the unnecessary and unjustified collection and online publication of personal data from overseas applications for domestic helper positions.
(iii) In December 2014, two travel agencies were directed to cease the collection and use of date of birth and identity card numbers from applicants joining their loyalty programme "

Alex Shepherd, Carolyn Bigg, Yang Xun and Aaron Patience, Partner, Managing Associate, Counsel and Managing Associate at Simmons & Simmons with the assistance of, and advice from, **JWS Asia Law Corporation and TMI Associates**

Japan

" Penalties may be imposed pursuant to the Act on the Protection of Personal Information Act (Act No. 57 of 2003) of Japan (PPIA). Under the PPIA, penalties are typically imposed as a result of a breach of an order issued by the relevant authorities following a breach of the PPIA (and not directly as a result of a breach the PPIA itself). Although results are yet to be published, it is unlikely that any penalties were imposed in 2014 "

Although the number of penalties issued last year is not easily ascertainable, recourse to the Japanese courts is also available through a civil cause of action with its basis in case law. This cause of action exists separately from the PPIA. Here, a victim of a privacy breach can bring a claim for a 'wrongful act' (fuhou koui) under Article 709 of the Civil Act of Japan (Act No. 89 of April 27, 1896) ('Civil Act').

Maximum potential penalty: Under the PPIA, a maximum fine of $2,490 may be imposed for the breach of an order issued by a government authority.
Maximum potential custodial sentence: Under the PPIA, six months imprisonment with labour may be imposed for the breach of an order issued by a government authority.

Notable case:

" In the ongoing Benesse case, an action under the Civil Act is being brought against Benesse Corporation ('Benesse'), a Japanese provider of educational services, regarding the misappropriation of personal information by an employee of a data processing company to which Benesse outsourced certain data processing functions. Reports suggest that over 20 million items of personal information may have been leaked from Benesse Corporation to brokers of name lists. The case, which is expected to be heard in in the courts this year, is significant given the number of plaintiffs involved: there have been reports of one class action campaign attracting 500 plaintiffs in two weeks "

Alex Shepherd, Carolyn Bigg, Yang Xun and Aaron Patience, Partner, Managing Associate, Counsel and Managing Associate at Simmons & Simmons with the assistance of, and advice from, **JWS Asia Law Corporation and TMI Associates**

Singapore

No. of penalties	Total amount	Average
3	$79,286	$26,429

Maximum potential custodial sentence: 12 month's imprisonment for making a request to obtain access to or change the personal data of another individual without the authority of that individual; knowingly or recklessly making a false statement to the PDPC; or obstructing or impeding the Commission or an authorised officer in the exercise of their powers or duties under the PDPA.

Notable case:

" In August 2014, a tuition agency and its director were each fined $29,449 for a total fine of $58,898 for failing to check the Do-Not-Call Registry before sending unsolicited telemarketing messages to Singapore telephone numbers belonging to individuals who registered on the Do-Not-Call Registry. This was the first successful prosecution for offences relating to the Do-Not-Call Registry. In October 2014, a property agent was fined $20,388 for sending unsolicited telemarketing messages to Singapore telephone numbers in breach of the Do-Not-Call provisions "

Alex Shepherd, Carolyn Bigg, Yang Xun and Aaron Patience, Partner, Managing Associate, Counsel and Managing Associate at Simmons & Simmons with the assistance of, and advice from, **JWS Asia Law Corporation and TMI Associates**

South Korea

The representative Korean Data Protection Authority is the Ministry of Government Administration and Home Affairs (MOGAHA). Other regulators in certain industry sectors (e.g., the Korea Communications Commission (KCC) in telecommunications industry, and the Financial Services Commission (FSC) and Financial Supervisory Service (FSS) in the financial service sector), are also in charge of data protection for users/customers in each such sector.

No. of penalties issued: 138 by the MOGAHA and 125 by KCC (based on our assessment of data from its press releases).
Total amount of penalties: Based on public information disclosed by KCC, a total of $581,025.
Biggest penalty issued: Among the representative cases disclosed by KCC, the largest fine imposed is an administrative penalty of $64,050 and an administrative fine of $13,725.
Maximum potential penalty: Under the Personal Information Protection Act (PIPA): a penalty of up to $91,500; an administrative penalty of up to $457,500; or an administrative fine of up to $45,750. Under the Promotion of Information and Communications Network and Protection of Information, etc. Act (ICNA): a penalty of up to $45,750; an administrative penalty of up to 3% of turnovers generated from businesses related to the violation, or if it is difficult to assess the turnovers, up to $366,000; or administrative fine of up to $45,750.
Maximum potential custodial sentence: PIPA: imprisonment (with forced labor) of up to 10 years. ICNA: imprisonment (with forced labor) of up to 5 years.

Notable case:

" A company ('Company-A'), a website operator, temporarily granted a user ID and a password to another company ('Company-B'), an outside service provider, to check the interoperability between the Company-A's website system and an outside website ('C-website'). After the check was conducted by Company-B, however, the temporary ID and password granted were not removed from the C-website. Thus, website users' personal data could be transmitted from Company-A's server to the C-website. Plaintiffs (i.e., users subscribing to the online service provided by Company-A via the C-website) claimed damages caused by the leak of their personal data. However, the Supreme Court of Korea has ruled that as it cannot be viewed that their data were leaked in this case.

The court's ruling is that there was no leak of personal data, so long as (i) the personal data in question were still in the possession of or under the control of Company-A, the pertinent online service provider, and (ii) no unauthorised third party had accessed or reviewed the data, even though Company-A was not fully compliant with certain statutory requirements for technical/administrative safeguards "

Sung Hey Park, Partner at Lee & Co

LATIN AMERICA

Argentina

No. of penalties

18

Biggest penalty

$2,421

Notable case:

“ On 26 March 2014, the Argentine Supreme Court provided its ruling on the protection of personal data and access to information in *CIPPEC v. Social Development Ministry*, Decree 1172/03. The Center for the Implementation of Public Policies Promoting Equity and Growth (CIPPEC) wanted information on how the Social Development Ministry allocated the public budget assigned by the Congress for specific social plans. The Social Development Ministry denied such information to the CIPPEC, stating that it could be understood as sensitive data (Section 16, paragraph I of the Appendix VII of Decree N° 1172/03 and Section 2, Personal Data Protection Act N° 25.326, 2000). The Ministry also stated that it was information that could lead to discrimination and could bring social injustice (according to the National Institute against Discrimination, Xenophobia and Racism).

Section 11 of the Act provides the general principle by which the communication of personal data is prohibited without the consent of the data holder, and provides some exceptions to this prohibition. As one of the exceptions, it foresees the possibility to assign personal data without the data holder’s consent when public interest is involved.

The Argentine Supreme Court stated that the prohibition to communicate personal data cannot apply when the public interest is at stake, by denying access to public information, since doing so obstructs the right to maximum disclosure of public information. Moreover, the Supreme Court stated that the fact that the information of the public registries involves third party data is not reason enough to impede its access. So, as long as the required information is not sensitive data (racial origin, political opinion, religious, philosophical or moral believes, union participation or information on sexual preferences or health), then the intimacy and honor of the involved persons is not affected by the disclosure of information relating to their social plans. Finally, the Supreme Court affirmed the need that the National Congress enact an Access to Information Act that clearly regulated the matter ”

Florencia Rosati and Manuela Adrogué, Senior Associate and Associate at Estudio Beccar Varela

Bolivia

“ To date, the right to privacy is not effectively enforced in Bolivia. The high financial cost of bringing a complaint, together with backlog and delay in the judiciary, generally discourage individuals from bringing suits to enforce this right. Although there have been several high-profile cases of alleged violations of the right to privacy over the course of the past year, no case resulted in a finding of a violation of the right to privacy ”

Lindsay Sykes and Gonzalo Iturry, Partner and Associate at Ferrere

Brazil

Biggest penalty $1,316,945

“ The Brazilian Ministry of Justice, one of the entities that has authority to investigate consumer related practices (including internet services, privacy and data protection matters), does not have the habit of imposing fines, even though it has triggered several investigations over the last few years. This is a direct consequence of the change towards privacy and data protection in the country, what even led to the approval of ‘Marco Civil,’ the Brazilian Internet Civil Rights Framework. But despite the long standing tradition of not applying fines to privacy related cases, last year, one the biggest Brazilian telecom companies was fined almost $1,316,945 for lack of transparency regarding its data processing activities.

In July 2014, the Department for Consumer Defense and Protection of the Brazilian Ministry of Justice fined ‘Oi,’ a Brazilian Telecom Company, $1,316,945 due to violations of principles enshrined in the Federal Consumer Code. During the investigation, it was possible to assess violations of the consumers’ right to information, privacy, intimacy and abusive advertisement. The telecom had partnered with a company in order to provide directed content and advertisement to its clients. It did so under the argument that the service would enhance users’ online experience. To perform the service, the company employed Deep Packet Inspection (DPI) techniques. All the user traffic was redirected to the company’s components installed on the ISP and then analysed to broaden users’ profile, which was then used to deliver directed content. But the ISP’s clients were not aware of such practice and had not authorised their content and personal data to be processed in such a way. Therefore, the Department held that there was a lack of transparency, prohibited the service, and applied the afore mentioned fine.

It is also worth noting that a new data protection law is currently being discussed, though it would take some years to come into effect ”

Renato Leite Monteiro, Attorney at Opice Blum, Bruno, Abrusio & Vainzof Advogados Associados

---

Colombia

No. of penalties	Total amount	Average
46	$711,518	$15,476

Biggest penalty $61,337

Maximum potential penalty: Non-compliance with the financial data protection regime may result in administrative sanctions that include: fines of up to approximately $363,518; suspension of the activities for up to 6 months; and/or closing of operations. Breach of the personal data protection regime, in turn, may result in administrative sanctions that include: fines of up to approximately $484,685; suspension of the activities related to processing of personal data; or temporary or immediate closing and/or termination of operations or activities related to processing of personal data.
Maximum potential custodial sentence: From a criminal perspective, as set forth in the Colombian Criminal Code, modified by Law 1273 of 2009, crimes may be sanctioned with imprisonment of between 4 to 8 years and fines of up to approximately $242,370.

Notable Data Protection Authority decision:

“ The biggest fine was equivalent to approximately $61,337. It was imposed on American System Service S.A.S., a company that provides English teaching services, for non-compliance with the financial data protection regime. The decision was based on the fact that the company did not keep copies or evidence of the authorisation granted by data subjects and did not implement procedures to inform data operators when the information is ‘in discussion’ with data subjects. Additionally, the company did not comply with the requirement of providing data subjects with a 20-day notice before reporting to the data operator any negative financial data about the breach of a contractual or financial obligation, in order to give them the opportunity to prove or make payment, as well as to controvert aspects such as the amount of the obligation and the date in which it became enforceable. In addition to the fine, the DPA ordered the company to carry out the necessary procedures before the data operator in order to eliminate any negative information reported without complying with the applicable requirements and warned it about its duty to comply with the breached obligations ”

Irene Velandia, Associate at Brigard & Urrutia

Costa Rica

Biggest penalty $17,020

Number of penalties issued: 4
Maximum potential custodial sentence: 3 to 6 years

“ Since the beginning, the Costa Rican Data Protection Authority (PRODHAB) has been working on the enforcement of the Protection in the Handling of the Personal Data of Individuals Law 2011 and despite the novelty of it, the PRODHAB has already imposed remarkable sanctions to companies that are infringing the Law. It has been only 4 sanctions, nonetheless the biggest fine imposed was about $17,020; very close to the biggest fine that can be imposed by the PRODHAB pursuant with our Law. As of July 2015, enforcement will be easier to carry out due to the expansion of the PRODHAB ”

Alejandra Castro and Valeria Agüero, Partner and Associate at Arias & Muñoz

---

Mexico

No. of penalties	Total amount	Average
7	$466,532	$66,640

Biggest penalty $280,665

Maximum potential penalty: According to the provisions of Article 64 of the Data Protection Act 2010, sanctions can range from 100 to 320,000 days of minimum wage in Mexico City depending on the type of offence set. In cases of sensitive personal data, such penalties may be increased to twice the amounts established. Considering that by July 2015, the minimum wage for the Federal District is $4.78 the maximum fine that could be imposed by the Authority can rise to approximately $3,061,408.
Maximum potential custodial sentence: 3 months to 3 years in prison for the person who, being authorised to process personal data for profit, causes a breach of security databases custody; and 6 months to 5 years when, in order to achieve an improper profit, the authorised person processes personal data by deception and takes advantage of the error. In cases of sensitive personal data, the penalties are doubled.

“ Of all the fines issued, only one has been paid. This is a fine imposed on a company in the textile sector (Creaciones Textiles de Mérida) for approximately $8,871.

The most sanctioned sector for violations of the Act has been the financial sector, followed by telecommunications, health and education.

Currently, a case that has grabbed the attention of the sector is the Google case. The Mexican National Institute of Transparency, Access to Information and Protection of Personal Data (INAI) followed the line of the European Court of Justice on the Right to be Forgotten, by considering Google responsible for the processing of personal data. Google Mexico argued that it is not the company that provides the service of search engine, but Google Inc., established in the United States and thus did not address the request to exercise the rights of the individual ”

Isabel Davara and Alexis Cervantes, Attorneys at Davara Abogados

Peru

No. of penalties	Total amount	Average
2	$78,860	$39,430

Biggest penalty $39,430

Maximum potential penalty: $133,210 (100 ITU tax units). This year it was established that the value of 1 ITU is around $1,332 per incurred violation of the law. In any case, the fine imposed may exceed 10% of the annual gross revenues received by the alleged offender during the previous year. Moreover, if the offender does not observe the obligations imposed by the Data Protection Authority, it could impose periodic penalty payments in the amount not exceeding 10 ITU.
Maximum potential custodial sentence: There is no criminal offense for violation of the Data Protection Law 2011. However, Article 157 of the Criminal Code provides for a criminal offense of abuse of computerised files holding sensitive information (imprisonment 2-4 years) and Article 154-A sanctions the illegal trafficking of personal data (2-5 years). Both offenses have been incorporated as cybercrimes.

“ The penalty issued to DatosPeru.org website, was a relevant one since it was the first company in Peru to be punished with a monetary fine by the DPA. Although the operator of the website was not identified, the sanction was issued. However, the site decided to end its activities due to its inability to pay the fine ”

Erick Iriarte and Cynthia Tellez, Head of Data Protection and Partner at Iriarte & Asociados

---

Uruguay

No. of penalties
15

Biggest penalty $2,398

Maximum potential penalty: $60,550 (500,000 Indexed Units).

“ In 2014 there were two fines of approximately $2,398. The first was for violation of the principle of prior consent for disclosure, as databases were provided for advertising purposes. The second penalty was for a company that violated the principle of purpose and prior informed consent ”

Ana Brian Nougrères, Director and Principal Consultant at Estudio Jurídico Brian & Associates

NORTH AMERICA

Canada

“ None of the Privacy Commissioners in Canada have issued fines (in some cases, it is not even within their powers to do so) in 2014 and there are a handful of cases (only 4), in which damages have been awarded and the amounts are relatively low.

While there were no cases in which penalties were awarded under the Quebec Privacy Act 1994, a penalty of $21,568 was issued under the Civil Code of Quebec in *Liboiron c. Banque de Montréal*. In this case, the Bank of Montreal ('BMO') reported the plaintiff's credit information to Equifax who in turn lowered her credit rating from R1 to R9. The client contested the amounts owed in court and eventually reduced her debt by a significant amount. Despite the plaintiff's numerous demands, BMO neglected to advise Equifax of the relevant changes pertaining to the plaintiff's credit information. Ultimately, the plaintiff was compensated for legal fees, loss of time, and other inconveniences.

In *Henry v. Bell Mobility*, a customer service representative from Bell Mobility revealed information concerning the plaintiff's account to an unauthorized third party. While the plaintiff alleged a loss of business opportunities as a result of the representative's actions, the Court stated that there was a lack of evidence in proving such a loss. Ultimately, the plaintiff was awarded $2,157 for the breach of information, and $862 for disbursements and legal costs under Personal Information Protection and Electronic Documents Act 2000.

In *Hopkins v. Kay* 2014 ONSC 321, the Ontario Court of Appeal held that the Personal Health Information Protection Act 2004 did not exclude the jurisdiction of the Superior Court form entertaining a common law claim for breach of privacy. The breach of privacy concerned in this case was the access of hospital records by a hospital staff without appropriate consent or other authorization. As a result, the Hospital was required to pay the plaintiff a sum of $20,704.

In *McIntosh v. Legal Aid Ontario*, the defendant illegally accessed the plaintiff's Legal Aid Ontario file for improper purposes. The files revealed that the plaintiff was involved with a Children's Aid file, and the defendant threatened to call the Children's Aid Society in an effort to have the plaintiff's children taken away from her. While the plaintiff claimed damages for several accounts, she was eventually awarded an amount of $6,470 due to a lack of evidence plus $5,608 in recovery costs inclusive of disbursements and HST under the tort of intrusion upon seclusion ”

Éloïse Gratton, Partner at Borden Ladner Gervais LLP

United States

" In 2014, the Federal Trade Commission (FTC) brought enforcement actions addressing a wide range of privacy issues, including spam, social networking, behavioral advertising, pretexting, spyware, peer-to-peer file sharing, children's privacy, Safe Harbor certification program violations, financial privacy, Do Not Call (DNC) and telemarketer violations, data broker violations, and mobile. Since 2002, the FTC's actions include over 130 spam and spyware cases, more than 40 general privacy lawsuits, over 50 security related enforcement actions, 119 DNC and telemarketer enforcement actions, more than 20 enforcement actions involving children's privacy, and more than 25 Safe Harbor settlements.

The FTC's principal tool to stop privacy and security violations and require companies to take affirmative steps to remediate deficiencies, is to bring an enforcement action under Section 5 of the FTC Act. That section allows the FTC to seek enforcement for deceptive or unfair trade practices. The FTC considers practices to be 'deceptive' if the company provides false or exaggerated statements about its privacy or security practices, which are not aligned with the practices that are actually in place. The FTC considers practices to be 'unfair' when the company fails to provide sufficient information to individuals about the collection, processing, sharing and security of their information. Most of the FTC's enforcement actions are brought under the 'deceptive' prong of Section 5.

The usual outcome of these enforcement actions is that the FTC and the organisation enter into a **20-year consent decree**. This settlement often includes, when appropriate, a requirement for the organisation to implement a comprehensive privacy and security program, biennial assessments by independent experts, monetary redress to consumers, disgorgement of ill-gotten gains, deletion of illegally obtained consumer information, and provision of robust notice and choice mechanisms to consumers. In some cases, the FTC has also required the company to pay for an on-site monitor to evaluate the company's compliance with the consent decree. Although the disgorgement fines can be significant, the major expense to the company generally comes from the costs associated with complying with the rigorous obligations in the consent decree, for 20 years, as well as the reputational damage to the company, loss of customers, and potential lawsuits. In some situations, the FTC has successfully put companies out of business based upon fraudulent or other prohibited practices.

If a company violates an FTC order including a consent decree, the FTC can seek civil monetary penalties for the violations, which can be up to **$16,000 per violation**. The FTC can also obtain civil monetary penalties for violations of certain privacy statutes, including the Children's Online Privacy Protection Act, the Fair Credit Reporting Act, and the DNC Registry.

The **largest DNC enforcement** in 2014 was a **$125 million** judgment against IAB Marketing Associates. The FTC alleged that the defendants operated a bogus trade association and tricked consumers into buying phony health insurance through deceptive telemarketing, including through illegal robocalls and illegal calls to customers who were registered on the DNC Registry. The settlement bans the defendants from selling healthcare-related products. The FTC agreed to suspend part of the monetary judgment (because the defendants are insolvent), but they were required to surrender assets valued at over $1,000,000, including $502,000 in retirement account funds and personal property that included five luxury cars.

With respect to **data security**, one example of FTC's enforcement in 2014 involved Snapchat, Inc., which settled charges that it deceived consumers with promises about the disappearing nature of messages sent through the service. Despite Snapchat's claims, the complaint described ways in which recipients could save snaps indefinitely. In addition, the FTC also alleged that the company deceived consumers over the amount of personal data it collected and the security measures taken to protect the same from misuse and unauthorised disclosure. The case alleged that Snapchat's failure to secure its Find Friends feature resulted in a security breach that enabled attackers to compile a database of 4.6 million Snapchat usernames and phone numbers. Under the terms of its settlement with the FTC, Snapchat is prohibited from misrepresenting the extent to which it maintains the privacy, security, or confidentiality of users' information. In addition, the company will be required to implement a comprehensive privacy program that **will be monitored by an independent privacy professional for the next 20 years**.

Similarly, an example of FTC's 2014 enforcement involving **children's privacy** involved Yelp, Inc., which agreed to settle charges that, from 2009 to 2013, the company collected personal information from children through the Yelp app without first notifying parents and obtaining their consent. When consumers registered for Yelp through the app on their mobile device, they were asked to provide their date of birth during the registration process. According to the complaint, several thousand registrants provided a date of birth showing they were under 13 years old, and Yelp collected information from them including, for example, their name, e-mail address and location, as well as any information they posted on Yelp. **Yelp paid a $450,000 civil penalty** "

Joan Antokol, Managing Partner at Park Legal LLC

CIS

Belarus

“ There is no specific Data Protection Authority (DPA) in Belarus. There are no special laws in Belarus that regulate liability for breach of personal data regulations specifically. Criminal and administrative offences codes provide for liability for violation of third parties’ rights in the sphere of informational relations (unauthorised access to computer information, illegal collection and distribution of information that relates to individuals’ private life etc), however there were no cases when unlawful processing of personal data was classified as a crime or administrative offence.

Personal data can be protected as a part of information regarding citizen’s private life. The Civil Code of the Republic of Belarus provides for a person’s right to protect his or her personal rights in court. A person whose personal rights have been violated may submit a complaint for compensation of losses. The amount of compensation is at the court’s discretion in each particular case. According to Belarusian court practice, courts generally refuse to require payment of such compensation (if a person did not actually suffer because of the breach), or require the respondent to make only a token payment. We are not aware of any cases of such complains that relate to unauthorised use of personal data ”

Yana Chirko, Associate at Dentons

Kazakhstan

Maximum potential penalty $7,603

Maximum potential penalty:

1. Illegal collection of information about the private life of individuals that is personal or family secret, without consent or causing substantial harm to rights and legitimate interests of an individual by illegal collection and (or) other processing of personal data entails a penalty from $4,344 to $7,603.
2. Failure to comply with measures on protection of personal data by a person, who is responsible for taking such action, if the act has caused substantial harm to the rights and legitimate interests of individuals may entail a penalty $7,603 to $10,861.
3. Actions envisaged in the first and (or) the second paragraph above, committed by a person using his official position or in order to benefit for themselves or for other persons or entities, as well as the dissemination of information referred to in the first part of this article, in public statement, publicly staged production or in the media may entail a penalty from $10,861 to $21,720 (Article 142 of the Criminal Code of the Republic of Kazakhstan).

Maximum potential custodial sentence:

1. Illegal collection of information about the private life of individuals that is personal or family secret, without consent or causing substantial harm to rights and legitimate interests of an individual by illegal collection and (or) other processing of personal data.
2. Failure to comply with measures on protection of personal data by a person, who is responsible for taking such action, if the act has caused substantial harm to the rights and legitimate interests of individuals may entail imprisonment for a term up to 3 years.
3. Actions envisaged in the first and (or) the second paragraph above, committed by a person using his official position or in order to benefit for themselves or for other persons or entities, as well as the dissemination of information referred to in the first part of this article, in public statement, publicly staged production or in the media may entail imprisonment for a term up to 5 years (Article 142 of the Criminal Code of the Republic of Kazakhstan).

Azim Usmanov, Partner at Colibri

Kyrgyzstan

Maximum potential penalty $1,698

Maximum potential penalty: For legal entities: Illegal accessing of legally-protected computer information (that is, information on machine-readable media, in computers, computer systems, and their networks), if this leads to destruction, blocking, modification, or copying of information, or the disruption of the work of the computers, computer systems or their networks may entail a penalty up to $1,698 (Article 409-2 of the Code on Administrative Liability of the Kyrgyz Republic).
Maximum criminal custodial sentence: Pursuant to the Criminal Code of the Kyrgyz Republic, illegal receipt of commercial or banking secrets may entail up to 5 years of sentence (Article 193 of the Criminal Code of the Kyrgyz Republic). Creation, use and distribution of malicious computer programs that lead to unauthorised destruction, blocking, modification or copying of information may entail a custodial sentence of up to 3 years (Article 290 of the Criminal Code of the Kyrgyz Republic).

Denis Bagrov, Partner at Colibri

Moldova

Maximum potential penalty $640

Maximum potential penalty: $640 and a prohibition to exercise a certain type of activity for up to 1 year. In all cases, fines must be confirmed by the courts.

“ In 2014, **55 administrative offences** have been identified, in respect of which **34 protocols** regarding breach of data protection legislation issued by the Moldovan Data Protection Authority. In accordance with local legislation, all such protocols were passed to the courts for judgment ”

Vladimir Iurkovski, Managing Attorney at Law at Schoenherr

Russia

Total amount
$169,442

Maximum potential penalty: Violation of the statutory procedure for collection, storage, use, or dissemination of information about citizens (personal data) entails imposition of administrative liability in the form of administrative fine of $171 for legal entities. A new draft bill, related to the liability for infringement of the legislation on personal data, is under consideration of Russian State Duma. This draft bill separates the administrative liability with regard to different grounds of violation of the law on protection of personal data and establishes new amounts of fines up to $5,121.
Maximum potential custodial sentence: In accordance with Criminal Code of the Russian Federation, the illegal collection or spreading of information about the private life of a person which constitutes his personal or family secrets, without his consent, or the distribution of this information in a public speech, in a publicly performed work, or in the mass media may entail the imposition of a custodial sentence of up to 2 years. The same offence committed by a person through his official position at work, could face imprisonment of up to 4 years.

Illegal accessing of legally-protected computer information (that is, information on machine-readable media, in computers, computer systems, and their networks), if this leads to destruction, blocking, modification, or copying of information, or the disruption of the work of the computers, computer systems or their networks, may entail the liability in a form of custodial sentence up to 2 years. The same act causing major damage (approximately $17,070 or more) could raise the sentence to 4 years.

Irina Anyukhina, Partner at ALRUD

Tajikistan

Maximum potential penalty $1,559

Maximum potential penalty: For legal entities: Failure to take measures ensuring the safety of storage and processing of information in establishments and entities irrespective of ownership, entailed theft, destruction or other consequences, in the absence of evidence of a crime may entail a penalty of up to $1,559 (Article 521 of the Code on Administrative Violence of the Republic of Tajikistan).
Maximum potential custodial sentence: Pursuant to Part 3 of Article 301 of the Criminal Code of the Republic of Tajikistan unauthorised copying or other misappropriation of the information stored in the computer system, network or on storage media, as well as the interception of information transmitted by using a computer connection committed with the purpose of obtaining particularly valuable information may entail a custodial sentence of up to 7 years.

Kerim Begaliev, Partner at Colibri

Ukraine

Maximum potential penalty $2,149

Maximum potential penalty: According to Article 188-39 of the Code of Ukraine on Administrative Offences, non-compliance with the order of personal data protection provided by the laws resulting in illegal access to such data or violation of data subject's rights, may entail a penalty amounting to up to $2,149.
Maximum potential custodial sentence: According to Article 182 of the Criminal Code of Ukraine, illegal collection, storage, usage, destruction, dissemination of the confidential information about a person, or illegal change of such information, may entail the imposition of a custodial sentence of up to 5 years.

" In Ukraine there is no similar public information (i.e. related to the number of penalties, average amount of fines, etc.). The Data Protection Authority (which functions are performed by the Human Rights Ombudsman) reports annually to the Parliament of Ukraine, but in those reports it does not provide any similar information "

Olga Belyakova, Senior Lawyer at CMS Cameron McKenna

Uzbekistan

Maximum potential penalty $9,760

There is no Data Protection Authority in Uzbekistan.

Maximum potential penalty: According to Article 191 of the Criminal Code illegal collecting, disclosure or use of information is subject to fines from $4,880 to $9,760 (100 to 200 of the minimum wage, which as of 29 June 2015 is $48.80).
Maximum potential custodial sentence: According to Article 191 of the Criminal Code illegal collecting, disclosure or use of information is subject to public works of up to 2 years, or imprisonment up to 6 months.

Dilshad Khabibullaev, Senior Managing Associate at Colibri

ACKNOWLEDGMENTS

EUROPE

AUSTRIA Dietmar Huemer, Partner at Legis
BELGIUM Tanguy Van Overstraeten and Clément Legrand, Partner and Associate at Linklaters LLP
BOSNIA & HERZEGOVINA Selma Šehović, Senior Associate at Marić & Co. LLC
CROATIA Marija Gregorić, Partner at Babić & Partners
CYPRUS Nicholas Ktenas, Partner at Andreas Neocleous & Co LLC
CZECH REPUBLIC Richard Otevřel and Petra Sochorová, Senior Associate and Counsel at Havel, Holásek & Partners
DENMARK Michael Hopp, Christian Wiese Svanberg and Christian Nielsen, Partner, Attorney and Paralegal at Plesner
ESTONIA Pirkko-Liis Harkmaa and Martin-Kaspac Sild, Partner and Associate at COBALT Legal
FINLAND Eija Warma,Counsel at Castrén & Snellman Attorneys Ltd
FRANCE Olivier Proust, Of Counsel at Fieldfisher
Florence Chafiol-Chaumont, Partner at August & Debouzy

GERMANY Andreas Splittgerber, Partner at Olswang
GREECE Maria Giannakaki, Attorney at Law, Karageorgiou & Associates
GUERNSEY Mark Dunster and Chloe Whitmore, Partner and Associate at Carey Olsen
HUNGARY Márton Domokos, Senior Associate at CMS Cameron McKenna LLP
ICELAND Ingvi Snær Einarsson, Attorney at Law at Lex
IRELAND John Whelan and Davinia Brennan, Partner and Associate at A&L Goodbody
ISLE OF MAN Data Protection Supervisor
ITALY Rocco Panetta, Partner at NCTM Studio Legale
Nadia Arnaboldi, Founder at Arnaboldi Corporate Firm
Garante per la protezione dei dati personali

LATVIA Ilze Bulkadere, Associate at Borenius
LITHUANIA Julius Zaleskis, Attorney at LAWIN
LUXEMBOURG Emmanuelle Ragot, Partner at Wildgen
MALTA Andrew Cauchi and Dr. Yanica Borg, Director of ICT Services and Lawyer at EMD (Malta)
THE NETHERLANDS Elisabeth Thole and Eva de Vries, Of Counsel and Attorney at Van Doorne
Jeroen Lub and Kevin Van 't Klooster, Partner and Associate at Osborne Clarke

NORWAY Øystein Flagstad, Partner at Advokatfirmaet Grette DA
POLAND Emilia Stępień, Founder at Law For Commerce Emilia Stępień Kancelaria Prawnicza
PORTUGAL Mónica Oliveira Costa, Partner at Coelho Ribeiro e Associados
SERBIA Uroš Popović, Partner at Bojović & Partners
SPAIN Laura Vivet, Partner at Conditio Iuris SLP
SWEDEN Henrik Nilsson and Sandra Lima, Partner and Associate at Gärde Wesslau Advokatbyrå
SWITZERLAND Jürg Schneider, Dr. iur., Attorney at Law and Partner at Walder Wyss Ltd
UNITED KINGDOM Hazel Grant, Antonis Patrikios and Samantha Sayers, Partners and Trainee Solicitor at Fieldfisher

ASIA PACIFIC

AUSTRALIA Alec Christie, IP/IT Data Privacy Law Partner at EY
CHINA, HONG KONG, **JAPAN**, **SINGAPORE** Alex Shepherd, Carolyn Bigg, Yang Xun and Aaron Patience, Partner, Managing Associate, Counsel and Managing Associate at Simmons & Simmons with the assistance of, and advice from, JWS Asia Law Corporation and TMI Associates
SOUTH KOREA Sung Hey Park, Partner at Lee & Co

LATIN AMERICA

ARGENTINA Florencia Rosati and Manuela Adrogué, Senior Associate and Associate at Estudio Beccar Varela
BOLIVIA Lindsay Sykes and Gonzalo Iturry, Partner and Associate at Ferrere
BRAZIL Renato Leite Monteiro, Attorney at Opice Blum, Bruno, Abrusio & Vainzof Advogados Associados
COLOMBIA Irene Velandia, Associate at Brigard & Urrutia
COSTA RICA Alejandra Castro and Valeria Agüero, Partner and Associate at Arias & Muñoz
MEXICO Isabel Davara and Alexis Cervantes, Attorneys at Davara Abogados
PERU Erick Iriarte and Cynthia Tellez, Head of Data Protection and Partner at Iriarte & Asociados
URUGUAY Ana Brian Nougrères, Director and Principal Consultant at Estudio Jurídico Brian & Associates

NORTH AMERICA

CANADA Éloïse Gratton, Partner at Borden Ladner Gervais LLP
UNITED STATES Joan Antokol, Managing Partner at Park Legal LLC

CIS

BELARUS Yana Chirko, Associate at Dentons
KAZAKHSTAN Azim Usmanov, Partner at Colibri
KYRGYZSTAN Denis Bagrov, Partner at Colibri
MOLDOVA Vladimir Iurkovski, Managing Attorney at Law at Schoenherr
RUSSIA Irina Anyukhina, Partner at ALRUD
TAJIKISTAN Kerim Begaliev, Partner at Colibri
UKRAINE Olga Belyakova, Senior Lawyer at CMS Cameron McKenna
UZBEKISTAN Dilshad Khabibullaev, Senior Managing Associate at Colibri

DataGuidance