GLOBAL PRIVACY ENFORCEMENT: Highlights and Trends

Research by OneTrust DataGuidance™

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

About the authors

OneTrust DataGuidance provides a suite of privacy solutions designed to help you monitor regulatory developments, mitigate risk, and achieve global compliance. With focused guidance around core topics, comparative Cross-Border Charts, a daily customised news service, and expert analysis, OneTrust DataGuidance provides industry leading solutions to design and support your entire privacy programme.

These tools, along with our in-house analyst service to help with your specific research questions, provide a cost-effective and efficient solution to design and support your privacy programme.

Website **www.dataguidance.com**

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

Introduction

Global Privacy Enforcement: Highlights and Trends features a variety of statistics including complaints and breach notifications received, investigations and enforcement notices issued, as well as further specifics on monetary penalties. All information included in this summary report is sourced from the OneTrust DataGuidance Enforcement and Breach project, created by the OneTrust DataGuidance in-house research team in collaboration with our network of experts. In particular, information outlined within this summary is compiled, where possible, from annual reports issued in 2018 by data protection authorities.

Full statistics in relation to each jurisdiction outlined within this report, as well as many more are available on the OneTrust DataGuidance platform.

How OneTrust DataGuidance helps

OneTrust DataGuidance offers a dedicated Enforcement and Breach Tracker which can be used by organisations to assess and compare enforcement actions taken by data protection and supervisory authorities in 2018 across countless jurisdictions.

In particular, our dedicated Cross-Border Chart provides the ability to compare complaints and breach notifications received, investigations and enforcement notices issued, across numerous jurisdictions and regions, as well as further specifics on monetary penalties issued.

In addition, corresponding Guidance Notes written by the OneTrust DataGuidance research team and our network of experts based locally in each jurisdiction, offer further detail on enforcement trends and the particular sectors impacted.

Organisations can also stay up-to-date in real-time with the latest enforcement actions and data breaches globally, as provided by our in-house research team.

Europe

The entry into force of General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR'), on 25 May 2018, created not only an increased awareness in data protection by organisations in terms of compliance but also triggered an increased willingness by individuals to submit complaints to data protection authorities, among other things. In Ireland for example, as confirmed by John O'Connor, Partner at William Fry, a total of 2,864 complaints were received by the Data Protection Commission ('DPC') over the course of 2018, 1,928 of which were made under the GDPR. Moreover, a total of 3,387 data breach notifications were received by the DPC under the GDPR with 2,429 emanating from the private sector. Similarly in Bulgaria, Mitko Karushkov and Mario Arabistanov, Partner and Senior Associate respectively of Kambourov & Partners, highlight that 693 complaints were received by the Commission for Personal Data Protection in 2018 with 534 being received after the entry into force of the GDPR.

From the statistics provided by 14 of the 16 Länder data protection authorities in Germany, a total of 29,000 complaints were received in 2018. In particular, the Data Protection Authority of Bavaria for the Private Sector received a total of 2,471 data breach notifications and issued a total of 10 monetary penalties. However, Baden-Württemberg data protection authority issued the highest recorded penalty of €80,000. Complete statistics for Lower Saxony for enforcement and breach are outlined on the following page.

Germany

Paul Voight, Partner at Taylor Wessing and the OneTrust DataGuidance research team have provided insight into all 16 Länder's data protection authorities and the specific enforcement actions of the same, accessible on the OneTrust DataGuidance platform.

Guidance Note: Lower Sawony - Enforcement and Breach

Introduction

Each Federal State in Germany has its own data protection authority, with the result that every year 16 reports are issued with respect to the different approaches each authority takes on the enforcement of data protection regulations. To highlight, 2018 was a year of change, as the GDPR entered into force.

The statistics provided by the 16 German state data protection authorities are not fully encompassing, therefore, it is to be expected that the reports of 2019 will provide more detail on the statistics given below and will show higher fines for breaches of data protection requirements.

This note outlines information on Lower Saxony data protection authority ('LfD Niedersachsen') as provided by its annual report 2017-2018.

Complaints received by data protection authority

Total No. received	1,000

Breach notification

Total No. received	370
Most common reporting sector	Information not available.

Enforcements notices

Authority	LfD Niedersachsen
Total No.	49
Most common sector	Information not available.

Monetary penalties

Authority	LfD Niedersachsen
Total No.	25
Highest	€2,250
Lowest	€2,250
Total amount	€36,000
Most common sector	Information not available.
Notes	The penalties were most commonly issued in relation to camera surveillance and noncompliance with rights of data subjects.

APAC

Approximately €1,065,610 worth of monetary penalties were issued by supervisory authorities in China, Australia, Malaysia, Singapore and Hong Kong for data protection violations over the course of 2018. The Personal Data Protection Commission in Singapore issued the highest recorded monetary penalty of €19,870 and the Korea Communication Commission ('KCC') issued the highest total amount of monetary penalties equalling approximately €710,170.

In addition, Australia and Hong Kong saw an increase in the number of complaints received over the course of 2018 in comparison to 2017. Across APAC, the most common reason for the submission of complaints, included, security of personal information; use or disclosure of personal information; and access to personal information.

Further information on complaints received by data protection authorities in Australia, South Korea, Hong Kong, and New Zealand are outlined below.

Australia

Angela Flannery, Partner at Holding Redlich, noted, "2017-18 saw an 18% increase in the number of privacy complaints received by the Office of the Australian Information Commissioner ('OAIC') as compared to the previous financial year. This, in the view of the Commissioner, reflected an increased awareness by Australians of their privacy rights and a greater willingness of Australians to take action to protect those rights. [...] Overall, 97% of privacy complaints were finalised by the OAIC within 12 months of receipt."

Guidance Note: Australia - Enforcement and Breach

Highlights: Complaints

Total No. received	2,947
Total No. resolved	2,766
Most common reason	The top 3 areas of complaint were: use or disclosure of personal information; security of personal information; and access to personal information.
Ave. time taken to resolve	3.7 months (this is the average time to resolve a complaint, not simply to respond to it).

South Korea

Kwang Bae Park and Michae Kang, Partners at Lee & Ko, provided detailed information in relation to enforcement in South Korea, highlighting, "Recently, Korea's data protection authorities (e.g., the KCC and Ministry of the Interior and Safety ('MOIS')) have been seeking to apply Korean data protection laws and regulations to foreign companies. Moreover, KCC and MOIS are actively investigating data breach incidents (incidents involving personal information of Korean data subjects) by foreign companies with businesses in Korea."

Guidance Note: South Korea - Enforcement and Breach

Highlights: Complaints

Total No. received	In 2018, the KCC received 57 personal information complaints.

New Zealand

June Hardacre, Senior Associate at MinterEllisonRuddWatts told OneTrust DataGuidance, "Under the Privacy Act 1993 ('the Act'), the Office of the Privacy Commissioner of New Zealand ('OPCNZ') has minimal enforcement powers and cannot:

- require agencies to give individuals access to information;
- require agencies to provide compensation to individuals; or
- require parties to accept a settlement offer or to accept the OPCNZ's findings.

In addition, there is no mandatory breach reporting regime under the Act and any reporting/notification of privacy breaches to either the OPCNZ or to impacted individuals is only do so on a voluntary basis."

Guidance Note: New Zealand - Enforcement and Breach

Highlights: Complaints

Total No. received	807
Total No. resolved	706
Most common reason	Access to information.
Ave. time taken to resolve	Less than six months.

Hong Kong

Mark Parsons and Anthony Lui, Partner and Associate respectively at Hogan Lovells LLP, told OneTrust DataGuidance, "The Office of the Privacy Commissioner for Personal Data ('PCPD') also received 1,890 complaints in 2018, which represents an increase of 23% from 1,533 complaints received in 2017. Among the private organisations subject to a complaint, the financial industry received the highest number of complaints (241 complaints), followed by the property management sector (166 complaints) and the transportation sector (166 complaints)."

Guidance Note: Hong Kong - Enforcement and Breach

Highlights: Complaints

Total No. received	1,890
Total No. resolved	The PCPD completed 1,751 complaint cases; accepted 844 cases for further handling; and made recommendations to the parties subject to a complaint in 686 cases.
Most common reason	Use of personal data without data subject consent.
Ave. time taken to resolve	Not applicable.

North America

OneTrust DataGuidance provides dedicated Guidance Notes outlining detailed statistics provided by top tier lawyers on the supervisory roles taken by the Federal Trade Commission ('FTC'), as well as the Office of Civil Rights ('OCR') within the United States Department of Health & Human Services ('HHS') and enforcement actions taken by both authorities over the course of 2018. Some information on key trends and highlights are outlined below.

USA

FTC

Alysa Z. Hutnik, Carmen Tracy and Khouryanna DiPrima, Partner and Associates respectively at Kelley Drye & Warrne LLP outline the FTC activities and comment, "The FTC's mission is to prevent anticompetitive, deceptive, and unfair business practices through law enforcement, advocacy, and education without unduly burdening legitimate business activity. One of the FTC's enforcement priorities is ensuring that consumers' personal information remains private and secure. To accomplish this mission, the FTC has brought over 100 cases against businesses that the FTC has alleged have failed to maintain reasonable privacy and data security practices. In 2018, the FTC brought six cases enforcing a range of privacy issues, including identity theft, data security, the Children's Online Privacy Protection Act of 1998 ('COPPA'), and alternative scoring related to one's credit. The FTC also referred two privacy and data security cases to the U.S. Department of Justice for litigation in which the agency intends to seek civil penalties."

OCR

Elizabeth Litten and Kristen Poetzel Ricci, Partner and Associate respectively at Fox Rothschild LLP, provide statistics on investigations and complaints submitted to and monetary penalties issued by the OCR within the HHS, among other things, and highlight, "The year 2018 hit a record high for the Health Insurance Portability and Accountability Act of 1996 ('HIPAA') investigations, triggered by the filing of over 25,000 complaints of HIPAA violations."

Guidance Note: USA - OCR - Enforcement and Breach

Highlights: OCR Penalties

Authority	HHS
Total No.	10
Highest	$16,000,000 (approx. €14,570,560)
Lowest	$100,000 (approx. €91,100)
Total amount	$28,683,400 (approx. €26,121,010)
Most common sector	Not applicable.
Notes	The University of Texas MD Anderson Medical Center: A U.S. Department of Health and Human Services administrative law judge ruled in favour of OCR and required MD Anderson to pay $4,300,000 (approx. €3,915,930) in civil penalties. The matter is under appeal.

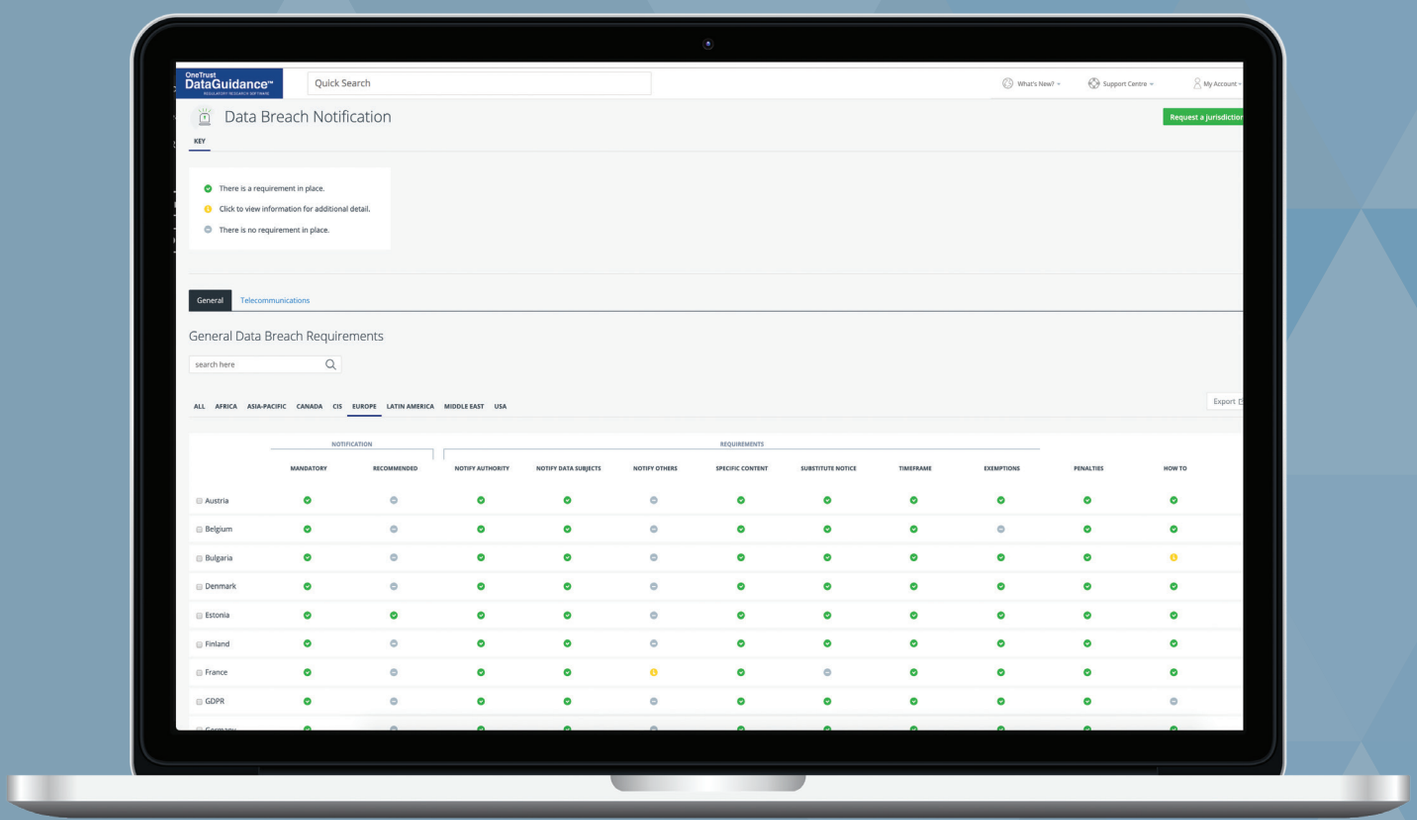
Global Regulatory Research Software

40 In-House Legal Researchers

500 Lawyers Across 300 Jurisdictions

With focused guidance around core topics, Comparison Charts, a daily customised news service and expert analysis, OneTrust DataGuidance provides a cost-effective and efficient solution to design and support your privacy program

- Legal Guidance & Opinion
- Law Comparison Tools
- Breach & Enforcement Tracker
- Ask-An-Analyst Service



SCAN TO ACCESS
FREE TRIAL
Use your camera or a QR code reader

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

South America

Supervisory authorities within Latin American jurisdictions, including Argentina, Columbia, Mexico, Peru and Brazil issued a number of enforcement actions in relation to data protection in 2018. The National Institute for Transparency, Access to Information and Personal Data Protection in Mexico for instance, issued approximately 97 enforcement notices and over €4 million in monetary penalties. Furthermore, the Peruvian data protection authority issued a total of 87 monetary penalties in 2018 most commonly directed at the retail sector.

Detailed information on monetary penalties in Argentina and Columbia are provided below.

Argentina

Diego Fernández, Partner at Marval, O'Farrell & Mairal, highlights, "Beside other sanctions and/or indemnification for damages derived from other applicable laws, such as general principles for damages contained in the National Civil and Commercial Code, the Argentina Data Protection Law authorises the Argentinian data protection authority ('AAIP') to apply the following penalties in the event of violation of the law: observation, suspension, fines of between ARS 1,000 (approx. €16) and ARS 100,000 (approx. €1,600) (which can go as high as ARS 3 million (approx. €47,930) when multiple violations are encompassed in the same proceedings), business closure, or cancellation of the file, record, or database.

Moreover, the AAIP can carry investigations ex officio or at the request of the parties in the private and public sector. Notably, the number of complaints filed with the AAIP is growing. It is expected that the proceeding inspections carried by the AAIP will continue growing during this year."

Guidance Note: Argentina - Enforcement and Breach

Highlights: Monetary Penalties

Authority	AAIP
Total No.	47
Most common sector	Telecommunications; banking; and technology.
Notes	Based on the number of infringements, the AAIP should have issued monetary penalties above the aforementioned highest penalty, but due to the cap imposed by Resolution No. 71 E/2016 ('Resolution 71'), fines were limited to ARS 3 million (approx. €48,050) as applicable to the specific type of infringement. Under Resolution 71, which caps the fines for the various infringements that it encompasses, applicable fines may not exceed ARS 1 million (approx. €15,980) for moderate infringements, ARS 3 million (approx. €48,050) for severe infringements, and ARS 5 million (approx. €79,890) for very severe infringements.

Colombia

The following stastics were provided by Andrés Fernández de Castro Muñoz, Senior Associate at Gómez-Pinzón Abogados.

Guidance Note: Colombia - Enforcement and Breach

Highlights: Monetary Penalties

Authority	Colombian data protection authority ('SIC')
Total No.	104
Highest	Information not available.
Lowest	Information not available.
Total amount	€2,420,980
Most common sector	Marketing or call center services; education; and retail.
Notes	According to the 2018-2019 Report, between 1 August 2018 and 31 July 2019, the SIC has imposed 104 monetary penalties for COP 8,990,650,270 (approx. €2,420,980) (page 15 of the 2018-2019 Report). However, it is not possible to access more detailed information about such figures. According to the 2011-2018 Report, between 1 January 2018 and 30 June 2018, the SIC imposed monetary penalties for COP 3,213,000,000 (approx. €866,550). However, it is not possible to access more detailed information about such figures.

CIS

From information available, data protection authorities located in the CIS had varied activity in 2018. In comparison to the Ukraine Parliamentary Commissioner for Human Rights ('the Commissioner') and the National Centre for Personal Data Protection ('NCPDP'), the Federal Service for the Supervision of Communications, Information Technology and Mass Communications ('Roskomnadzor') issued the highest number of monetary penalties, enforcement notices, and initiated the highest number of investigations. In particular, Roskomnadzor had more than 40,000 complaints in comparison to the 806 received by the Commissioner.

The sectors most commonly issued enforcement notices by the Commissioner, the NCPDP and Roskomnadzor also varied significantly in 2018. For example, the Commissioner issued enforcement notices most commonly to the railway and postal sector, whereas Roskomnadzor most commonly issued such notices to website providers and the financial sector.

Further information on the enforcement notices issued by the Commissioner, the NCPDP, and Roskomnadzor is provided below.

Russia

Irina Anyukhina, Partner at ALRUD Law Firm, provides detailed analysis in our Russia – Enforcement and Breach Note on the Roskomnadzor activities over the course of 2018.

Anyukhina outlines, "In 2018, Roskomnadzor paid close attention to the processing of personal data on the internet. In particular, the Government approved the Decree of the Government of the Russian Federation of 13 February 2019 No. 146 on Approval of the Rules for the Organization and Implementation of State Control and Supervision of the Processing of Personal Data, Which Allow Roskomnadzor to Carry Out Supervisory Measures By Way of Monitoring Companies Activities on the Internet or Analysing Available Information About Their Activities. Further to monitoring, Roskomnadzor may decide to conduct an unscheduled inspection of the company, order to rectify revealed violations, and impose an administrative fine."

Guidance Note: Russia - Enforcement and Breach

Highlights: Enforcement Notices

Authority	Roskomnadzor
Total No.	6,419 administrative offences and 768 orders to rectify the violation.
Most common sector	Website providers and financial sector.

Common violations

- failure to file notification with Roskomnadzor on the processing of personal data;
- failure to provide information to Roskomnadzor;
- failure to implement legal, organisational and technical measures on protection of personal data; and
- failure to ensure appropriate legal grounds to personal data processing.

Ukraine

Olga Belyakova, Partner at CMS Cameron McKenna Nabarro Olswang LLP provides analysis on enforcement notices issued and investigations initiated by the Commissioner on the next page.

Guidance Note: Ukraine - Enforcement and Breach

Highlights: Enforcement Notices

Authority	The Commissioner
Total No.	45*
Most common sector	Railway; and post.
	*45 enforcement notes mentioned above relate to notices to address infringements of the Law of 1 June 2010 No. 2297-VI on Personal Data Protection (as amended). The majority of actions by the Commissioner relate to public sector.

Moldova

Marina Zanoga, Partner at ACI Partners LLC, summarises the enforcement actions of the National Centre for Personal Data Protection ('NCPDP').

"In the last few years, there has been a consistent trend of the NCPDP increasing activity; 2018 was not an exception. As result of the extensive awareness actions deployed by the NCPDP, and media coverage on the importance of the protection of personal data and the safeguarding of personal life, the complaints submitted to the NCPDP have increased in volume and diversified.There is a constant 'evolution' of the type of complaints submitted to the NCPDP. Thus, besides the increased number of complaints, their nature has significantly changed. The complaints envisage new segments of personal data protection and refer to processing of personal data by the mass-media, processing of medical data, as well as the processing of minors' personal data."

Guidance Note: Moldova - Enforcement and Breach

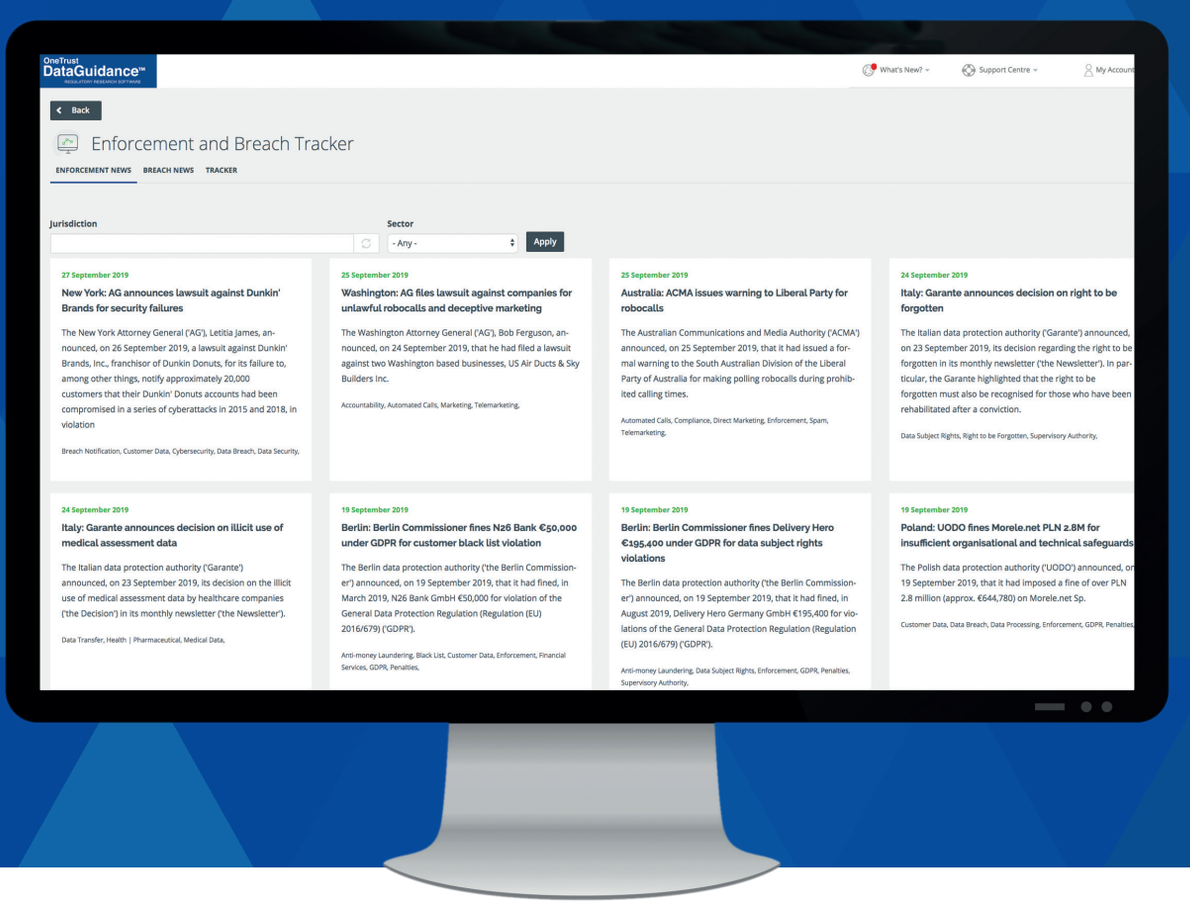
Highlights: Enforcement Notices

Authority	NCPDP
Total No.	191
Most common sector	Information on where in the private sector enforcement notices were most frequently issued is unavailable.
Notes	According to the Report of the NCPDP for the year 2018, the most common enforcement notices were issued for breaches of data processing requirements in the following areas: processing personal data through video surveillance; processing personal data belonging to minors; processing consumers' personal data, among others.

NEW
Enforcement and Breach Tracker

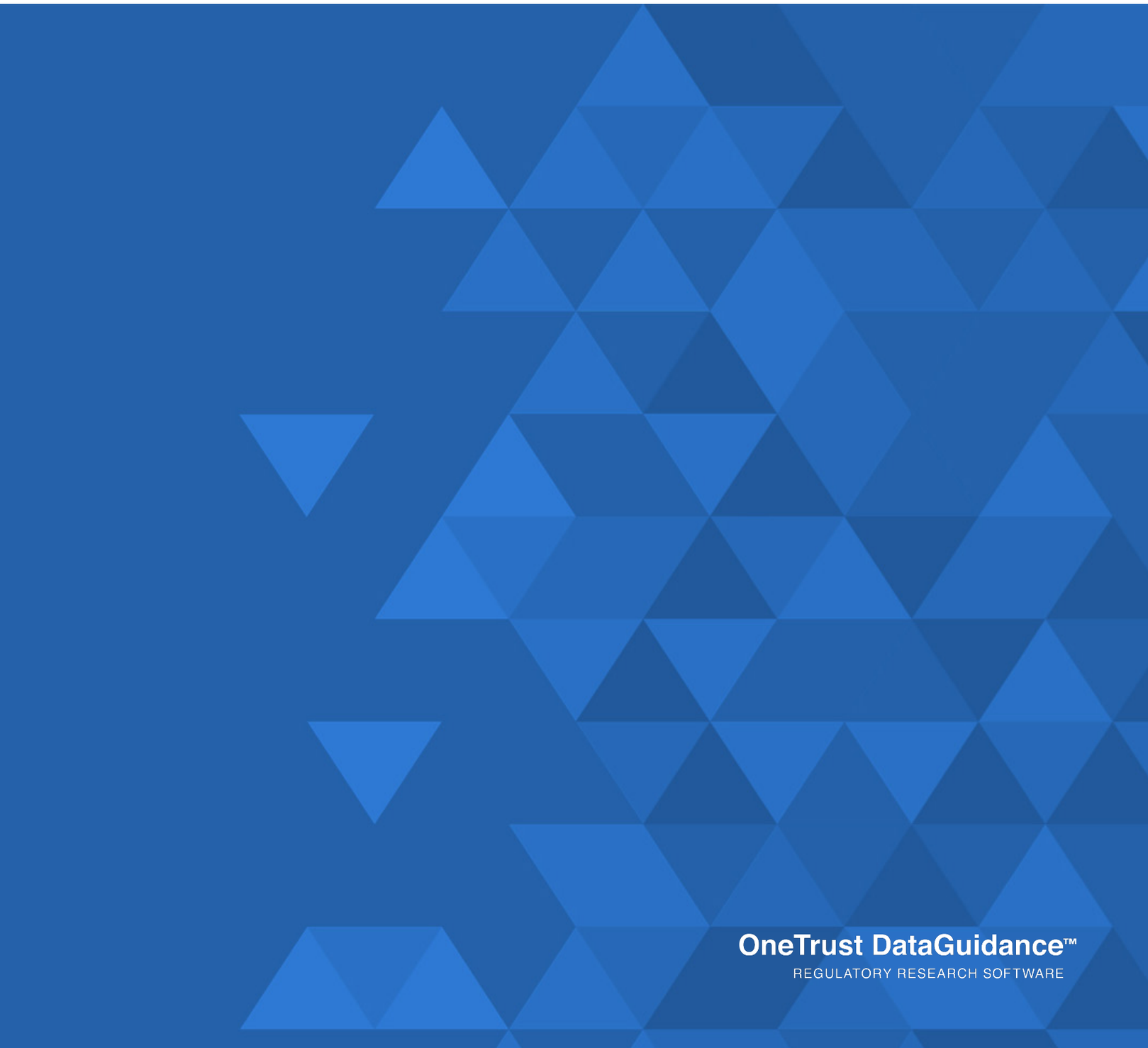
Leverage data to assess privacy and data protection risk with our Enforcement and Breach Tracker. Stay up to date and compare across numerous jurisdictions and sectors when it comes to:

- Numbers of complaints
- Investigations
- Data breaches
- Enforcement actions
- Monetary penalties



SCAN TO ACCESS
FREE TRIAL
Use your camera or a QR code reader

OneTrust
DataGuidance™
REGULATORY RESEARCH SOFTWARE


OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE