Data Protection Day - Key developments and trends for 2023

28 January 2023 is Data Protection Day (or Data Privacy Day outside of Europe), which marks the anniversary of the Council of Europe's Convention 108.

To mark Data Protection Day 2023, Baker McKenzie's Global Data Privacy and Security Team is pleased to present this special edition update of key data protection and privacy developments and trends across the globe, as well summarising future legislative changes, predictions, and enforcement priorities to look out for during 2023.

International data transfers continue to be a significant area of focus, particularly from an EU perspective. The practical implications of the Schrems II judgment are still being felt by organisations and grappled with by data protection authorities, and related developments are on the horizon with the recently published draft adequacy decision for the EU-US Data Privacy Framework (you can read more in our update here). There are emerging trends in enforcement action from EU data protection authorities shining a light on issues such as transparency and privacy notice information, as well as the legal basis for processing personal data, particularly in the context of online behavioural advertising.

Outside of the EU, there is a proliferation of new privacy laws and amendments to existing privacy laws to keep up with. These range from new laws (or amendments to existing laws) which have now come into force, laws or amendments that are expected to come into force this year, as well as discussions or proposals for future reforms. In particular, there are developments to be aware of in Australia, Japan, Taiwan, Vietnam, India, Qatar, UAE, Saudi Arabia, Türkiye, Canada, Argentina, Vietnam, Switzerland, several US states and the UK. Almost half of these are G20 economies so we except such changes will be important given the inextricable link between information driven trade ecosystems.

Children's personal data continues to be high up on the agenda across the globe. In the UK, this is reflected in the ICO's Age Appropriate Design Code, and in the US, with the California Age-Appropriate Design Code Act (you can read more in our update here). Children's online safety is also an important topic of wider focus in addition to data protection, and you can read more about this in our specially commissioned report "Online child safety: an opportunity to get it right" led by Elizabeth Denham of Baker McKenzie and produced jointly with Milltown Partners (available here).

You can find more information on these developments and trends and many others in our summary below. You can also jump to specific country overviews using the links below.

If you have any specific questions, please do not hesitate to get in touch with your usual Baker McKenzie Data Privacy and Security contacts.

Europe

Middle East

UK

UK Data Protection Reform

Following a public consultation process which took place in 2021, the Data Protection and Digital Information Bill ("DPDI Bill") was published in July 2022. However, the DPDI Bill has not yet progressed further through the legislative process. Therefore, the proposals in the DPDI Bill may change if and when the DPDI Bill progresses through Parliament.

In summary, one of the Government's key objectives with the DPDI Bill is to reduce the perceived compliance burdens on organisations by removing or replacing certain obligations, particularly record keeping obligations. Proposed amendments include removing the requirement for a DPO to be mandatory, changing records of processing obligations, changing requirements regarding data protection impact assessments, as well as removing the requirement to appoint a UK representative under Article 27 of the UK GDPR if an organisation outside of the UK is directly subject to the UK GDPR because it offers goods or services to data subjects in the UK or monitors the behaviour of data subjects in the UK.

The proposals are not a wholesale replacement of the UK GDPR, but are instead an incremental shift away from, in the UK Government's view, perceived "box ticking" exercises and unnecessary administrative burdens in certain areas.

There are also proposals to expand the circumstances where consent is not required for placing cookies, for example, by expanding the list of circumstances where cookies are regarded as "strictly necessary".

You can read more detail about the proposed UK reforms and the DPDI Bill in our update here.

International Data Transfers

UK Addendum and IDTA: As of 21 September 2022, for new contracts which involve the transfer of personal data to jurisdictions that are not deemed to be adequate under the UK GDPR, the International Data Transfer Agreement ("IDTA") or the UK Addendum to the EU Standard Contractual Clauses should now be used.

For agreements that were entered into before 21 September 2022 on the basis of the previous EU Standard Contractual Clauses approved under the Data Protection Directive ("Directive SCCs"), these continue to be valid for the purposes of the UK GDPR until 21 March 2024, provided the processing operations and the subject matter of the contract remain unchanged, and reliance on those Directive SCCs ensures that the transfer of personal data is subject to appropriate safeguards. You can read more about this in our update here.

ICO Guidance and Transfer Risk Assessment Tool: The UK Information Commissioner's Office ("ICO") published new guidance and resources on data transfers in November 2022, including a new transfer risk assessment tool. The ICO's guidance and transfer risk assessment tool adopts a different approach from the European Data Protection Board's ("EDPB") recommendation on supplementary measures, although the ICO has stated that, from a UK perspective, organisations can either follow the ICO's approach in the TRA tool, or the EDPB's approach. You can read more about this in our update here.

Future Adequacy Regulations: The UK Government has stated that it intends to expand the list of jurisdictions that are recognised as adequate for the purposes of the UK GDPR by issuing its own adequacy regulations post Brexit. The UK Government has a list of priority jurisdictions for these adequacy assessments. The top priority jurisdictions are Australia, Colombia, the Dubai International Financial Centre, Singapore, the US and South Korea. There are also longer-term priority jurisdictions which include India, Brazil, Indonesia and Kenya.

As of 19 December 2022, adequacy regulations under the UK GDPR in relation to South Korea are now in force. This is the first new adequacy regulation issued under the UK GDPR for one of the Government's "priority" jurisdictions. Although the European Commission adopted an adequacy decision in relation to South Korea in December 2021, this did not apply under the UK GDPR as it was

adopted after the Brexit transition period ended. The European Commission's adequacy decision does not cover the processing of personal credit information under the Act on the Use and Protection of Credit Information by controllers that are subject to oversight by the Financial Services Commission (credit rating agencies, banks, insurance companies etc). However, the UK's adequacy regulations are broader that the European Commission's adequacy decision and also cover credit information processed by controllers subject to oversight by the Financial Services Commission.

ICO25 and future regulatory approach

On 14 July 2022, the ICO published its three year plan, ICO25, which sets out how the ICO will prioritise its work and regulate over the next three years.

ICO25 includes an action plan for the ICO's focus areas, which includes areas intended to empower people such as:

- reviewing the impact of "predatory marketing calls";
- reviewing the use of "algorithms within the benefits system";
- reviewing the impact the use of "AI in recruitment could be having on neurodiverse people or ethnic minorities, who weren't part of the testing for this software;" and
- "ongoing support of children's privacy" which involves continuing to enforce the ICO's Children's Code.

You can read more in our update regarding ICO25 here.

In November 2022, the ICO also set out a new strategic approach to regulatory action, for example, opting to use reprimands instead of fines on public sector organisations, with all reprimands now being published on the ICO's website.

The ICO has also started to publish a list of data protection complaints from data subjects, a list of self reported personal data breaches by data controllers and a list of incidents and investigations regarding cyber attacks. These lists date back to Q4 2020 and were not previously published on the ICO's website or publicly available.

Children's Personal Data

Organisations have been required to comply with the ICO's Age Appropriate Design Code since 2 September 2021. The Code applies to online services "likely" to be accessed or used by a child, which for these purposes is anyone under the age of 18.

As mentioned in ICO25, the processing of children's personal data continues to be a focus area for the ICO.

The ICO has been proactive in reaching out to organisations in certain sectors to understand what compliance steps are in place to meet the requirements of the Code. This approach is likely to continue. For example, in September 2022, the ICO stated that it is looking into several different online services and their conformance with the Code as well as ongoing investigations.

Argentina

2022 was an important year for data protection in Argentina, and much more is expected for 2023.

Last year started with the appointment of Ms. Beatriz de Anchorena as the new Director of the Argentine Data Protection enforcement authority, the Access to Public Information Agency ("AAIP" for its acronym in Spanish).

In line with the commitments she made during her candidacy, Ms. de Anchorena initiated the process of updating the Personal Data Protection Act (enacted in 2000). The aim is to be in a position to address the new challenges posed by advances in technology and the development of the digital economy, as well as harmonisation with regional and international standards from a human rights perspective. The proposal for the new law presented by the AAIP expressly contemplates extraterritorial application. The modernisation process included the opening of a public consultation on the draft bill inviting scholars, organisations, and other interested parties to submit their comments and opinions on the proposal. At present it is not clear when the draft bill will be discussed by congressmen and women or if it will be included in their short-term agenda.

In 2022, Argentina also ratified Convention 108+ on the Protection of Individuals with regard to the Automatic Processing of Personal Data. Argentina was the second Latin American country (following Uruguay) to ratify the Convention. This is aligned with the goal of helping Argentina maintain its EU adequacy decision, which is key for international data transfers, attracting investments and conducting business.

Most of the sanctions imposed by the AAIP in 2022 were related to breaches of the security duty, with the authority focusing its investigations on the lack of implementation of adequate technical and organisational measures to prevent and/or mitigate the effects of a data breach. Despite this, there is currently no explicit legal obligation under Argentine law to report a security incident/data breach, the AAIP simply recommends doing so and considers it best practice. We anticipate AAIP will become more interested in cybersecurity and related data protection safeguarding matters.

Australia

After a slow start, there were some sudden and important changes to Australia's privacy laws in 2022, but more active enforcement and wider-ranging reform proposals are expected in 2023…

2022: the calm and then the storm

At the start of 2022, it was expected that the government of the day would introduce an Online Privacy Bill to parliament, which would have made a number of changes to the *Privacy Act 1988* ("Privacy Act"), including significantly increasing maximum penalties for non-compliance. Following the mid-2022 federal election, however, the Online Privacy Bill lapsed and was not resurrected by the new Labour government. Meanwhile, privacy practitioners waited patiently for the Attorney-General to complete the lengthy and much overdue review of the Privacy Act.

All seemed relatively quiet on the privacy front until late in the year, when a flurry of high profile cyber-attacks and privacy breaches prompted the new government to increase funding for Australia's privacy regulator, the Office of the Australian Information Commissioner (OAIC), and urgently rush amending legislation through parliament aimed at encouraging better privacy practices and enabling the OAIC to respond more effectively to non-compliance.

The expedited regulatory changes commenced on 13 December 2022 and are outlined here. The most important changes were:

- **Increases to the maximum penalties** for serious or repeated interferences with an individual's privacy. Most significantly, the potential maximum liability for corporates is now

set at the greater of: (a) AUD 50 million, (b) three times the value of the benefit obtained from the contravention, if this can be ascertained, or (c) if the court cannot determine the value of the benefit obtained, 30% of the body corporate's adjusted turnover during the "breach turnover period" (being not less than 12 months).

- **Expanded powers for the OAIC**,including powers to request more information and documents about an entity's compliance practices and to direct complaint respondents on rectification compliance failures. The regulator now also has greater abilities to share information with other regulatory authorities, make certain disclosures and publications in certain circumstances, and issue infringement notices with monetary penalties attached for failure or refusal to comply with requests to provide information, answers or records.
- **A revision of the test for extra-territorial application of the Privacy Act**, which means that the regulator only needs to demonstrate that an overseas entity is carrying on business in Australia in order to enforce the Privacy Act against it.

As regards the ongoing review of the Privacy Act, by the end of the year, it was unofficially reported in the media that the review was complete, and that a report on its findings had been handed to the government.

2023: change is coming

The media has suggested that the Privacy Act review report and associated government response will be published in the first half of 2023. In late December 2022, the Attorney-General tweeted of an intention to overhaul the legislation in 2023, reinforcing this in January 2023 with remarks confirming that there will be a "whole range of modernisations of the Privacy Act".

Some uncertainty remains regarding exact timeframes and next steps.

Nevertheless, it seems reasonable to expect that the report will be published fairly soon and that the government will announce associated reform proposals, with a view to revamping the regulatory regime in 2023.

Potential reform ideas discussed in the 2021 discussion paper for the review included:

- various changes to enforcement and remedies including increases in and additions to penalties (note that these proposals were made prior to the 2022 reforms), and a direct right of action for individuals and potentially a statutory tort for invasion of privacy;
- broadening key definitions (e.g. "personal information" will clearly include certain technical and inferred information) and adding new definitions for concepts which currently only have regulatory guidance as to their meaning (e.g. "reasonably identifiable", "consent");
- amendments to requirements for collection practices, privacy notices and consents, including:
    - pro-privacy default settings on a sectoral or other specified basis;
    - an express requirement that privacy notices must be clear, current and understandable, and stronger requirements for when a notice is required; and
    - the development of a code to introduce standardised layouts, wording, icons, and/or consent taxonomies.

- additional requirements and prohibitions relating to certain large scale or high risk acts and practices (e.g. direct marketing; use of sensitive information, children's personal information, location data or biometric data; automated decision making with legal or significant effects), and further protections for children and vulnerable individuals;
- express rights for an individual to object or withdraw their consent to the handling of their personal information, and to request erasure of personal information in certain circumstances; and
- various changes relating to overseas disclosures including a new mechanism to prescribe certain jurisdictions and certification schemes as substantially similar to the Australian Privacy Principles and the development of standard contractual clauses for entities to use when disclosing personal information overseas.

While there is no concrete indication of which of the review's proposals will be adopted, Australia's privacy regulator has generally expressed approval for the proposed reforms and, with cyber-attacks and ransomware becoming ever more prevalent and significant threats, public sentiment seems to be swinging in favour of more stringent privacy regulation.

It therefore seems likely that 2023 will mark the start of a major shift in Australia's privacy laws, if not a wholesale revolution. Businesses should watch closely for the release of the report on the Privacy Act review, and be ready to digest and make submissions on any draft legislation that is released. Additionally, we expect the OAIC to be increasingly active in its policing of compliance with the Privacy Act throughout 2023, emboldened and empowered by the 2022 reforms and its increased funding. As a result, it is now more critical than ever that businesses have stringent compliance measures in place and are ready to respond to data breaches and regulatory requests for information.

Austria

Continuing hot topic: The practical application of Schrems II

In a landmark decision issued in January last year, the Austrian Data Protection Authority ("DPA") issued the first major decision in Europe after *Schrems II* dealing with international data transfers from the EU to the US. In this declaratory decision, the DPA reasoned that the transferred data (the specific cookies, title of a visited website and date and time of a visit and browser-related information such as screen resolution and language settings) would qualify as personal data as they would make the user "distinguishable", which the DPA essentially equated with "identifiable". If the IDs stored in the cookies were combined with the browser-related data and the IP address, this would (in the DPA's opinion) result in a digital fingerprint that would qualify as personal data in any case. Further, the DPA argued that US intelligence authorities could identify the data subject anyway. Without considering the practical risk or practice of US authorities, the DPA then found that widely used supplementary measures to ensure an adequate level of protection of personal data would not be sufficient.

Even though the DPAs in the EU were planning to take a coordinated approach to the more than 100 similar complaints lodged throughout the EU that was hashed out by a taskforce of the EDPB, so far, only the French and Italian DPAs adopted essentially the same position as the Austrian DPA. The DPAs of Spain and Luxembourg, however, dismissed complaints because the website operators had already removed the cookies in question.

The Austrian and French decisions have been appealed and are not yet final. It remains to be seen whether the appeals courts will side with the DPAs or take a different approach.

Hot topic for 2023: Consequences of sending mass cease-and-desist letters with damages claims based on the GDPR

In the latter half of 2022, on behalf of their client, an Austrian lawyer sent demand letters to at least 10,000 small Austrian businesses. With each letter, the lawyer claimed immaterial damages of EUR 100 and costs of EUR 90 based on the argument that the businesses had disclosed their client's IP address to a third party via a tool embedded on their websites and thereby "massively annoyed" their client and caused "considerable discomfort". The lawyer filed two lawsuits as "test cases". The massive volume of websites concerned and other circumstantial evidence suggests that the claimant may not have accessed the websites, but rather used some kind of crawler to directly target websites using the tool in question. The implications of this will have to be assessed not only by the civil courts concerned with the lawsuits, but also by the Public Prosecutor in a criminal investigation against the lawyer and their client.

Austrian DPA issues FAQs regarding cookies

The Austrian DPA has issued "FAQs on the subject of cookies and data protection" (German only) on its website. In its otherwise rather general answers, the Austrian DPA also touches on the permissibility of "pay or okay" models whereby users can either pay money for access to a website or give their consent to the use of cookies (usually advertising cookies for the display of personalised advertising). According to the Austrian DPA, "pay or okay" models are permissible in principle and payment for access to a website can be an alternative to consent if the following is met:

- Full compliance with data protection;
- No exclusivity with regard to the content or services offered, i.e. companies with an explicitly public (utility) mandate or universal service providers cannot permissibly use "pay or okay";
- No monopoly or quasi-monopoly position in the market;
- A reasonable and fair price for the pay alternative;
- No processing of personal data for the purpose of personalised advertising if a user chooses the pay alternative.

Whistleblower Protection Act expected in Q1 of 2023

A draft law transposing the EU Whistleblower Protection Directive (Directive (EU) 2019/1937) is currently being reviewed by the Austrian legislator. The final law, the Whistleblower Protection Act ("*HinweisgeberInnenschutzgesetz*" or "*HSchG"*) is expected to take effect in Q1 of 2023. Based on the current draft whose material scope of reportable breaches is kept to a minimum, it appears that companies will have to deal with two whistleblowing regimes in Austria: the one within the scope of the new HSchG and one outside its scope. This will, in particular, also require differentiation regarding the legal basis of any data processing, the applicability of any data subject rights and the necessity of works council agreements and privacy impact assessments.

Belgium

The Belgian DPA has been very active in 2022, including:

- carrying out investigations, especially with respect to the use of cookies, and imposing sanctions such as reprimands, warnings, fines, etc. relating to non-compliance with the GDPR;
- investigating and following-up on personal data breaches;
- issuing opinions on draft bills involving the processing of personal data; and
- implementing its strategic and operational objectives of its 2020-2025 Strategic Plan into concrete objectives.

Processing of sensitive personal data, the legitimacy of the processing and online collection of personal data using cookies and similar technologies, especially in the context of the adtech industry, have been particularly scrutinised by the Belgian DPA in 2022.

Enforcement

- In February 2022, the Belgian DPA found that IAB Europe's Transparency and Consent Framework (TCF), which facilitates the management of users' preferences and consents in relation to online personalised advertising (in particular in the context of Real Time Bidding), infringed several provisions of the GDPR. The Belgian DPA therefore imposed a EUR 250,000 fine on IAB Europe and ordered the company to present an action plan to bring its activities into line with the GDPR within two months. IAB Europe appealed the decision of the Belgian DPA before the Brussels Market Court, which decided in September 2022 to refer preliminary questions to the Court of Justice of the EU ("CJEU"). The preliminary questions notably concern IAB Europe's status of (joint) controller with respect to processing activities carried out in the context of the TCF as well as whether a "TC String" (i.e. a character string that captures the preferences of an Internet user in connection with the processing of his or her personal data in a structured and machine-readable manner) constitutes personal data within the meaning of the GDPR. The case is currently pending before the CJEU (Case C-604/22). In addition, on 11 January 2023, the Belgian DPA informed IAB Europe of the formal approval of its action plan to bring its activities into compliance, which means that IAB Europe now has up to six months to implement the suggested measures.
- Also in February 2022, the Brussels Market Court referred another preliminary question to the CJEU in a case involving the publication, requested by a public notary in accordance with the law, of certain personal data in the Belgian Official Gazette. The questions mainly concern the qualification of the Official Gazette as data controller and is currently pending before the CJEU (Case C-231/22).
- In April 2022, the Belgian DPA imposed fines on the Zaventem and Charleroi airports of EUR 200,000 and EUR 100,000 respectively, as it found that temperature checks which were put in place in because of the Covid-19 pandemic and involved the processing of passengers' health data did not rely on a valid legal basis under the GDPR. Both airports appealed the decisions of the Belgian DPA before the Brussels Market Court, which partially annulled them in December 2022. The Court mainly found that the Belgian DPA did not sufficiently consider several mitigating factors mentioned in Article 83 GDPR when deciding the amount of the fines imposed, and therefore reduced the fines to EUR 50,000 for the Zaventem airport and EUR 25,000 for the Charleroi airport.
- Following a large-scale investigation by the Belgian DPA regarding the use of cookies on the most popular Belgian press websites, in May and June 2022 the Belgian DPA imposed two

fines of EUR 50,000 each on two press groups for non-compliance with the information and consent requirements in relation to cookies.

Belgian DPA's key priorities for 2023

The Belgian DPA has defined its key priorities for 2023, which revolve around cookies, the role of the DPO, data protection in the context of the development of the "smart city" and continued control actions with respect to data brokers.

Brazil

In 2022, the protection of personal data has been recognised as a fundamental individual right by an amendment to the Brazilian Federal Constitution, while the Brazilian DPA ("the ANPD") has been granted more autonomy and has been converted into an autarchy (similar to an agency, with more independence).

On an administrative level, the ANPD has been active in issuing regulations, guidance and public consultations, as well as addressing incidents involving personal data that need to be notified according to the law. With a significant increase in the number of cyberattacks, there has been an increase in notifications to the ANPD, as well as governmental initiatives to publish sector-specific regulations on cyber security, with more to come.

The ANPD was previously associated with the Federal Presidency but has now been transferred to the organisational chart of the Ministry of Justice as of January 2023, although it still maintains independence. The ANPD disclosed a revised regulatory agenda for 2023 and 2024, with the main regulatory priorities for 2023 including:

- Regulation on application of administrative sanctions;
- Data subjects rights;
- Security incident notification requirements;
- International transfers of personal data;
- Personal Data Protection Impact Assessments;
- The role of the "Person-in-Charge" (similar, but not totally equivalent, to the role of a data protection officer);
- Legal bases for the processing of personal data;
- Definition of high-risk and large-scale processing activities;
- Processing of sensitive personal data by religious organisations;
- Use of personal data for academic purposes and for carrying out studies by a research body;
- Anonymisation and pseudonymisation procedures; and
- Regulation of processing of personal data for research purposes.

Under Brazilian law, enforcement of data protection rights is not limited to the ANPD. Companies can also be subject to individual or collective claims for failure to comply with Brazilian General Data Protection Law ("LGPD"), by data subjects or associations and other authorities representing a group of data subjects seeking indemnification or other measures. Since the enactment of the LGPD, there

has been an increase in consumer, civil and employment litigation involving data protection matters, and we expect that cyber security litigation, as well as consumer and employment disputes involving personal data, will continue to increase.

Canada

In Canada, privacy laws are enacted at the federal and provincial/territorial level, and are applicable to private sector entities, public sector entities, and health information custodians. In 2022, there were notable legislative and policy developments to modernise and reform private sector privacy legislation at the federal level and in the Province of Quebec, which will carry-over into 2023.

Federal

In June 2022, the federal government introduced Bill C-27 (Digital Charter Implementation Act, 2022) to overhaul and modernise the current private sector privacy regime under the Personal Information Protection and Electronic Documents Act (PIPEDA). Bill C-27 proposes the following new laws:

- **Consumer Privacy Protection Act:** If passed, this new law would repeal a part of PIPEDA and replace it with a new legislative regime, to govern the collection, use, and disclosure of personal information for commercial activity in Canada. This new law would provide:
    - heightened data protection measures for individuals with respect to their right to request, access, delete and transfer their personal information;
    - enhanced data breach reporting, breach notification, and security safeguard requirements for organisations;
    - new privacy protections for minors, such as limitations on the collection and use of a minor's personal information and higher standards for organisations to meet in handling a minor's personal information;
    - broader regulatory powers for the federal privacy regulator, the Office of the Privacy Commissioner of Canada (OPC); and
    - significant fines for non-compliance of up to 5% of global revenue or $25 million, whichever is greater, for the most serious offences.
- **Artificial Intelligence and Data Act (AIDA):** Currently, there is no AI specific legislation in Canada. If passed, AIDA would require organisations that design, develop and use AI systems to identify, assess, manage, and mitigate risks and biases associated with high-impact AI systems. AIDA introduces new criminal prohibitions and penalties related to the use of unlawfully obtained data for AI development, instances where the careless deployment of AI systems poses serious harm, and where there is fraudulent intent to cause substantial financial loss through the deployment of the AI system.
- **Personal Information and Data Protection Tribunal Act:** If passed, this new law would establish a new regulatory authority, the Personal Information and Data Protection Tribunal, which would play a role in the enforcement of the Consumer Privacy Protection Act. This new authority would be able to impose administrative monetary penalties, as well as, upon the request of organisations and individuals, review decisions of the Office of the Privacy Commissioner of Canada (OPC).

In the coming year, Bill C-27 will continue undergoing legislative review. If this legislation is passed, the OPC will be significantly engaged in developing and implementing transitional measures for the

new privacy requirements. The OPC may also consider the development of regulatory tools and enforcement mechanisms for the new privacy measures. Private-sector organisations will also need to assess, revise, and update their privacy practices and policies in relation to the new privacy requirements.

Quebec

The first phase of amendments introduced by Bill 64, an Act to modernise legislative provisions as regards the protection of personal information, to the private sector privacy legislation in Quebec, an Act Respecting The Protection Of Personal Information In The Private Sector, came into force on 22 September 2022. As of this date, organisations are required to appoint an internal privacy officer and notify Quebec's privacy regulator, the Commission d'accès à l'information du Québec, of any data breach that presents a "risk of serious injury" to an individual.

In the coming year, organisations will need to comply with the second phase of amendments by 22 September 2023. Organisations are required to: (i) establish and implement data governance policies; (ii) perform a privacy impact assessment before transferring personal information outside of Quebec; (iii) inform data subjects when automated decision-making and profiling technologies are being used; (iv) abide by enhanced consent requirements, including clear, free, and informed consent relating to a specified purpose and timeframe; (v) develop an external privacy policy in clear and plain language; (vi) implement "privacy by default" to products and services offered to the public; and (vii) destroy or anonymise personal information once the original purpose has been fulfilled.

The last phase of amendments related to data portability will come into force on 22 September 2024, through which individuals can request that an organisation disclose their personal information to another individual or business. In the coming year, the Commission d'accès à l'information du Québec will continue to monitor an organisation's compliance with and enforce provisions under the amended Act Respecting The Protection Of Personal Information In The Private Sector. Private sector organisations will need to ensure that they are complying with the updated and new privacy requirements ahead of the various enforcement dates (as set out above).

Colombia

The Colombian DPA (i.e. the Superintendence of Industry and Commerce – "SIC"), was very active during 2020 and 2021, issuing orders and opening investigations particularly against companies engaged in digital services whose activity grew exponentially during the Covid-19 pandemic. Although the SIC's activity was not as intense in 2022, perhaps given the changes in the leadership of the agency's data protection team, there were still several interesting developments in Colombia.

In February 2022, the Colombian Ministry of Commerce, Industry and Tourism issued Decree 2555 of 2022, which regulates the recognition of Binding Corporate Rules in Colombia. The Binding Corporate Rules are self-regulatory systems adopted by a business group, which are put in place by the controller of personal data established in Colombia, to facilitate the transfer of personal data to other controller(s) located outside the national territory and that are part of the same business group.

In 2022, the SIC also fined the largest Latin American marketplace for exposing customers data. In this case, an employee of the company sent a promotional email to several customers, which exposed to all the email addresses, names, and surnames of the recipients. This information was used by unauthorised third parties to contact these individuals with unsolicited messages.

The SIC also sanctioned a major financial services firm. According to the authority, the financial services company systematically disregarded complaints from citizens related to the use of their personal financial information. In its decision, the agency issued a general warning to companies that process personal data in the financial services industry, advising them to adopt measures to ensure such issues do not occur in the future.

The SIC opened an investigation on the largest company in the Colombian aerospace sector after reaching a preliminarily conclusion that the carrier collected personal data through its applications using mechanisms that the SIC considered to be illegitimate. The SIC continues to focus on digital service providers. In one decision, the agency imposed an order on a tech company not domiciled in Colombia on the basis that cookies were used to collect data from Colombian users. The company has since challenged the decision.

Czech Republic

Amendments to the Czech Telecommunications Act entered into force in 2022. These amendments implemented the opt-in consent requirement for cookies under the ePrivacy Directive, aligning the Czech cookie rules with the EU requirements. In addition, the amendments significantly changed the rules for telemarketing in the Czech Republic (generally, opt-in is now required). The Czech DPA jointly with the Czech Telecommunication Office, has published detailed guidance on the new telemarketing rules. Around 800 complaints have already been submitted to the Czech Telecommunication Office as the competent authority supervising compliance with the telecommunication rules. The first fine for a breach of the new telemarketing rules was issued in 2022 for CZK 420,000 (approximately EUR 17,500).

The Czech DPA has been active in 2022 with investigations and publishing guidance. During its investigations, it has focused on cookies, smart quarantine and direct marketing, as well as processing relating to offers of goods and services. It also inspected processing activities relating to audio-visual recordings in a business establishment and processing by the executor's office. In the first six months of 2022, the DPA concluded 11 investigations relating to the GDPR and five investigations relating to the sending of commercial communications. While the highest fine imposed by the DPA for a GDPR breach is CZK 2,000,000 (approximately EUR 83,400), in 2022 the DPA only imposed four enforceable fines, the highest of which amounted to CZK 70,000 (approximately EUR 3,000).

In 2023, the DPA plans to investigate the following in relation to the private sector:

- processing personal data by a significant processor and the involvement of sub-processors, including changes to sub-processors as well as compliance with the contractual provisions under Article 28(3) and (4) GDPR and documenting audits carried out;
- processing personal data in connection with telemarketing, in particular whether personal data is lawfully processed and whether transparency obligations are complied with;
- processing of personal data by employers in attendance systems, in particular regarding categories of personal data processed, retention periods and purpose limitation;
- processing of personal data in a database, in particular regarding sources of personal data, legal basis for the processing as well as transparency and handling of data subject rights;
- sending commercial communications via SMS.

Jointly with other European authorities, the DPA will also participate in an investigation within the EDPB Coordinated Enforcement Framework concerning data protection officers. In addition, the DPA plans to carry out various investigations in relation to the public sector, including Eurodac, processing during the visa process, CCTV system with biometric functions by a public body as well as processing by police. We expect to see more enforcement actions and fines from the DPA in 2023.