

International Data Protection Update

WINTER 2021/2022

MARCH 10, 2022



This Update highlights some of the international data protection issues that caught our attention and the attention of our clients over the winter, including updates on European data transfers and cookie compliance, regulatory enforcement actions, and data protection laws in Canada, China, India and Saudi Arabia.

AUTHORS

Andreas Kaltsounis
akaltsounis@bakerlaw.com

Melinda McLellan
mmclellan@bakerlaw.com

Nichole Sterling
nsterling@bakerlaw.com

CONTENTS

Europe and Commonwealth of Independent States

Russia's Attack on Ukraine
EU's Data Governance Act
EU and UK Data Transfer Updates

Cookie Compliance

European Data Protection Board Guidance

Other New Data Protection Laws and Regulations

Middle East and Africa

Saudi Arabia's Personal Data Protection Law

United Arab Emirates Federal Law on the Protection of Personal Data

Other New Data Protection Laws and Regulations

Asia-Pacific

China's Personal Information Protection Law

India's Data Protection Bill

South Korea's Adequacy Decision

Americas

Quebec's Bill 64

Uruguay's New Personal Data Transfer Rules for the United States

Update from the Brazilian Data Protection Authority

Selected Enforcement Actions



Europe and Commonwealth of Independent States

Russia's Attack on Ukraine

Government [cybersecurity agencies worldwide](#) are urging all organizations to bolster online defenses, adopt enhanced cybersecurity postures and be prepared to respond to disruptive cyber activities. At this time, no specific and credible cyberthreats are being reported in the United States, but [destructive malware](#), [ransomware](#) and [targeting of network infrastructure devices](#) have been reported in Ukraine. Building on increased fear of cyberattacks in the United States, the Senate rushed through new legislation to strengthen the federal government's defenses and to mandate incident reporting by certain entities in U.S. critical infrastructure. BakerHostetler's [Digital Risk Advisory and Cybersecurity team](#) is actively advising clients on emerging threats and associated government action related to the war in Ukraine.

EU's Data Governance Act

In November 2021, the European Parliament and the European Union Member States [reached agreement](#) on the European Commission's proposed [Data Governance Act](#), concluding the required [trilogue negotiations](#). Unlike the EU's General Data Protection Regulation (EU GDPR), the Act's applicability is not limited to personal data. The Act [aims to promote](#) the sharing of all data "across sectors and Member States." Balancing this broader use of data are privacy-enhancing measures to increase public trust in data sharing, such as the use of secure processing environments, anonymization, data intermediary licensing, and restrictions on the transfer of nonpersonal data outside the European Union. The remaining steps for the Act's entry into force are likely to be completed this spring, with full compliance required by the summer of 2023. Already moving forward with the next piece in its [strategy for "Shaping Europe's digital future,"](#) the European Commission [introduced the European Data Act](#) on February 23, 2022.

EU and UK Data Transfer Updates

Last September, all older versions of the EU standard contractual clauses (SCCs) were repealed. Moving forward, cross-border personal data transfers relying on SCCs must now use the [new SCCs issued in June 2021](#), and transfers still covered by the expired SCCs must transition to the new forms by December 27, 2021. However, there remained a UK-sized hole in the complex European data transfer matrix. In early February, the United Kingdom's Information Commissioner's Office (ICO) sent two

documents to Parliament – (1) the revised [international data transfer agreement](#) (IDTA – like SCCs, but with a clearer name) and (2) a separate [Addendum](#) for use with the EU SCCs. Assuming Parliament makes no objections, these documents will become final and enforceable on March 21, 2022. The ICO has indicated that companies may begin using these documents now, but it also plans to provide more guidance for their use soon.

Meanwhile, data protection authorities (DPAs) throughout the EU have been throwing wrenches into personal data transfer compliance efforts. Notably, the first couple of [NOYB's post-Schrems II data transfer complaints](#) have finally been resolved. In January, the Austrian DPA, the Österreichische Datenschutzbehörde, [decided](#) that a health information portal could not continue its use of analytics cookies that were relaying user information to the United States. The decision broadly defined personal data and found that the supplementary measures put in place by the analytics provider were ineffective to safeguard against the specific personal data transfer risk gaps identified. Also in January, the European Data Protection Supervisor (EDPS) published a [similar decision](#) regarding the use of data analytics on a European Parliament website. Following these decisions, several other DPAs (including [Denmark](#), [France](#), the [Netherlands](#) and [Norway](#)) adopted analogous decisions or released revised guidance related to the use of website analytics. These decisions and commentary are steadily eroding confidence in the utility of the supplementary measures identified by the European Data Protection Board (EDPB) in its [guidance from last June](#) on personal data transfers, particularly calling into question the effectiveness of certain uses of encryption and pseudonymization, transparency reporting, additional technical measures, and organizational processes as means for limiting public authority access to personal data.

In addition, the EDPS [published the final report](#) from its study on government access to data in third countries (specifically China, India and Russia – none of which fared well in the report). The German Data Protection Conference (Datenschutzkonferenz) [released an expert opinion](#) on the current state of U.S. surveillance law and authorities; it had commissioned the expert opinion to answer questions related to the risk of continued personal data transfers to the United States. The report takes an extremely broad view of which U.S. organizations might be deemed electronic communication service providers subject to FISA Section 702, which could affect how German authorities assess personal data transfers. The Irish Data Protection Commission's decision on personal data transfer issues raised in the Schrems II case [may soon see resolution](#). The EU and U.S. governments continue to actively negotiate a new Privacy Shield framework, which both agree is a high priority, but the United States [seems more bullish](#)

on the potential for a replacement in the near future [than the EU](#), according to recent statements from both.

Cookie Compliance – Germany’s Federal Act on the Regulation of Data Protection and Privacy in Telecommunications and Telemedia, which regulates data in accordance with the EU’s ePrivacy Directive, entered into force on December 1, 2021, and [ushered in revised cookie guidance from Germany’s DPAs](#). A month later, 2022 opened with more supersized cookie fines – €210 million [split between two companies](#) – issued by the French DPA (the Commission nationale de l’informatique et des libertés or CNIL) for cookie noncompliance. France’s Conseil d’État [validated a previously challenged cookie fine](#), finding that the one-stop-shop mechanism of the EU GDPR did not apply to violations of the ePrivacy Directive as transposed into French national law. Accordingly, the CNIL can issue cookie violation fines to companies with lead supervisory authorities in other Member States.

[Guidelines](#) from Italy’s DPA (Garante), which were released last summer, [went into effect](#) as of January 9, 2022, and are included in the Garante’s 2022 [proactive investigation plan](#). Luxembourg [issued guidelines for cookies and tracking technologies](#) in October 2021, and the [Czech Republic](#) provided guidance on cookies and consent along with its recently implemented [opt-in requirement for cookies](#). Not to be left out, Turkey’s DPA (Kişisel Verileri Koruma Kurumu) [released draft cookies guidelines](#) for public comment in January. Alongside these guidelines, several EU Member States have prioritized proactive cookie audits of major websites operating in their countries. [Cyprus](#), [Denmark](#), [France](#) and [Latvia](#), for example, released information about their cookie audits, highlighting that many companies audited were not in compliance with various cookie requirements. NOYB continues its cookie monitoring activities and announced on March 4 that it [had sent another round of draft complaints](#) to website operators regarding noncompliant cookie banners.

European Data Protection Board Guidance – On November 18, 2021, the EDPB adopted its [new draft guidance](#) on the interplay between Article 3 of the EU GDPR (territorial scope) and Chapter V of the GDPR (transfer restrictions). This new guidance specifies that personal data processing by organizations in countries outside the European Economic Area is governed by the transfer restrictions of Chapter V, even when the organization is subject to the GDPR through the law’s extraterritorial applicability. But the EDPB unhelpfully leaves open the question of how to comply with Chapter V in such circumstances, acknowledging that the required transfer tools are currently “only available in theory,” leaving open [the possibility that more SCCs may be in the works](#) to help fill this gap.


In the past few months, the EDPB adopted several other new guidance documents, including new [guidelines on the right of access](#), revised [data breach notification examples](#), updated guidelines on using [Codes of Conduct as personal data transfer tools](#), and final guidelines on when [individual rights may be restricted under GDPR Article 23](#) for purposes such as national or public security. The EDPB’s [cookie banner taskforce](#) has been set up specifically to coordinate the response to cookie banner complaints that NOYB has filed with many DPAs. Further, the EDPB [issued a statement](#) calling for regulatory cooperation and the consistent application of existing laws that protect individual data protection rights in response to the Digital Services Package and Data Strategy proposed by the European Commission. As part of this statement, the EDPB asked for targeted advertising that relies on individual tracking to be phased out and ultimately prohibited.

Other New Data Protection Laws and Regulations

- **Andorra** – In October 2021, Andorra [amended its Personal Data Protection Act](#) with the amendments set to take effect in May 2022. The changes largely harmonize Andorra’s existing law with the EU GDPR, introducing or updating legal bases, individual rights, controller and processor obligations, data breach notification requirements, and data transfer restrictions.
- **Belarus** – Belarus’ [Law No. 99-Z on Personal Data Protection](#) became effective on November 15, 2021. The law broadly follows the transparency, legal basis, processing limitation and freely given consent obligations of the EU GDPR and provides individuals with the rights to access, correct and delete personal data. Noncompliance with the law can result in administrative, civil and criminal penalties.

Middle East and Africa

Saudi Arabia’s Personal Data Protection Law – In September 2021, Saudi Arabia issued the [Personal Data Protection Law \(PDPL\)](#), which is broadly similar to the EU GDPR and will come into effect on March 23, 2022. The PDPL will apply to the processing of personal data of any Saudi resident, regardless of citizenship, and to any personal data processing, regardless of location. Individual rights include access, amendment and deletion rights similar to those in the EU GDPR, as well as the right to be informed of the purpose, legal basis and practical justification for personal data processing at the time of collection. The PDPL appears to restrict personal data transfers outside Saudi Arabia; however, forthcoming regulations are expected to provide details regarding data transfer and localization requirements. Data controllers must pay a fee and register their data processing activities with the [Saudi Data &](#)



[Artificial Intelligence Authority](#) (SDAIA), and foreign companies will need to appoint a local representative. Controllers are required to implement appropriate technical and organizational measures to safeguard personal data, and in the event of a personal data breach the controller may be required to notify SDAIA and affected individuals. Fines for noncompliance with the PDPL may be up to SAR 3 million (approximately US\$800,000) and can include imprisonment for up to two years.

United Arab Emirates (UAE) Federal Law on the Protection of Personal Data

UAE's [Federal Decree-Law No. 45 of 2021](#) on the Protection of Personal Data [was announced](#) last fall. It took effect January 2, 2022. Additional executive regulations are expected soon, after which organizations will have six months to comply with the law and regulations. The law applies to controllers and processors located both in the UAE and outside the UAE that process the personal data of individuals located in the UAE. Note that the law exempts the free zones already subject to their own data protection laws, including the Dubai International Financial Centre and the Abu Dhabi Global Market, and personal data covered by sector-specific data protection legislation, such as health and financial data.

Under the new law, personal data [should be processed](#) in a fair, transparent and lawful manner in line with the principles of purpose limitation, data minimization, accuracy, security, confidentiality and storage limitation. The new law provides individuals with rights to access, correct and delete their personal data, as well as rights to restrict and object to personal data processing. Personal data may be transferred internationally (1) with the data subject's consent; (2) to countries approved by the UAE Data Office (regulations enumerating these countries have not yet been released); (3) to countries that have a data protection agreement with the UAE; and (4) under certain other exceptions that will be set forth in the regulations. Data breach notification is required under the new law. The UAE Data Office has been established as the data protection authority responsible for monitoring compliance, issuing guidance, accepting complaints and proposing new legislation.

Other New Data Protection Laws and Regulations

- **Botswana** – Botswana's [Data Protection Act, 2018](#) came into effect October 15, 2021. Organizations have a one-year transition period to comply. Under the law, organizations are obliged to process data in a lawful, transparent and fair manner that incorporates purpose limitation, security and data minimization principles. Individuals have rights to access, correct and delete personal data and can object to or restrict data processing. Penalties include fines up to BWP 1 million (approximately US\$86,000) and imprisonment up to 12 years.


- **Oman** – Oman's [Law on the Protection of Personal Data](#) was issued on February 9, 2022, and will be in effect on February 9, 2023. Although further executive regulations are pending, the new law replaces the limited privacy obligation previously contained in Oman's Electronic Transactions Law. The new law provides individual privacy rights and relies heavily on transparency and explicit and documented consent.
- **Rwanda** – Rwanda's [Law No. 058/2021 Relating to the Protection of Personal Data and Privacy](#) was published on October 15, 2021. Organizations that currently process personal data in Rwanda have a two-year transition period to comply, but organizations that begin new personal data processing in Rwanda must comply immediately. Data subjects have rights to access, erase and correct personal data and can object to and restrict personal data processing. Organizations that wish to process personal data must register with the National Cyber Security Authority. Noncompliance may result in the cancellation of data processing registration, fines up to 5 percent of the annual turnover and up to 10 years' imprisonment.
- **Zimbabwe** – Zimbabwe's [Data Protection Act](#) was published on December 3, 2021, imposing data minimization, transparency and purpose limitation obligations on controllers and providing data subjects with rights to be informed of the processing of, access, object to processing of, and correct and delete personal data. The Act created the Data Protection Authority and criminalizes certain offenses related to the unlawful acquisition of, interference with and disclosure of personal data. Violating the Act can lead to fines and imprisonment.

Asia-Pacific

China's Personal Information Protection Law (PIPL)

China's [PIPL](#) took effect on November 1, 2021. PIPL is a national law intended to synthesize obligations for processing personal information in mainland China. PIPL consists primarily of statements of principle and broad pronouncements of rules (discussed in our [Summer 2021 International Data Protection Update](#)) with details to be filled in by regulations and agency interpretations, which have been slowly rolled out. Businesses subject to PIPL should also be aware of local or regional requirements, such as the [Shanghai Data Regulations](#) and [Shenzhen Special Economic Zone Data Regulations](#), which impose local requirements relating to data security, the use of facial recognition technology and data subject rights.

On October 29, 2021, the Cyberspace Administration of China (CAC) [released draft measures](#) for [assessing outbound data transfers](#) in compliance with PIPL, the Chinese [Cybersecurity Law](#) and the



Chinese [Data Security Law](#). PIPL and other Chinese data protection laws already include strict requirements for cross-border transfers of personal information, with the general expectation that personal information relating to Chinese persons will remain localized in China. Personal information transferred abroad may require a security assessment that is then reported to the CAC to facilitate both prior and continuous regulatory supervision. This security assessment is separate from other types of required assessments, such as a data protection impact assessment or transfer self-assessment. The draft measures indicate that the security assessment will at a minimum require a declaration, a self-assessment report regarding the proposed outbound data transfer, and copies of any relevant contracts between the data exporter and the data importer.

Two weeks later, on November 14, 2021, the CAC issued draft regulations addressing [network data security management](#). These regulations address many of the same topics as PIPL and other Chinese data protection laws but add detail regarding data breach notification, vendor management, the cybersecurity review process and the protection of personal information generally to guide businesses seeking to comply with these laws. The regulations propose a 72-hour notification period for personal data breaches that cause harm but include an eight-hour notification period for data security incidents affecting 100,000 or more individuals. Businesses cannot process personal information without consent, unless the personal information is required to provide a service. Consent logs related to sharing personal information must be maintained for five years. These regulations also address cross-border data transfers by placing limitations on the personal information that may be transferred, requiring contractual provisions and allowing for individual complaints related to data export. Businesses exporting Chinese personal information and other important data must keep a log of their data exports (which must be maintained for three years) and file an annual report with the CAC identifying key information about the data exports.

Since November, the CAC has also issued draft [network security review measures](#) applicable to businesses operating in the critical information infrastructure space; [administrative measures](#) for businesses marketing financial products online; and [regulations on the management of mobile application information services](#), such as the provision of voice calling, live broadcasting, instant messaging and hosting or publishing.

India's Data Protection Bill

On December 16, 2021, India's Joint Parliamentary Committee established to review the draft [Personal Data Protection Bill](#) finally [submitted its report and revised draft of the Bill](#), ending more than two years of deliberations. [Key changes in the report](#)

include a phased two-year implementation period, the inclusion of protections for nonpersonal data, a 72-hour data breach-reporting obligation for both personal and nonpersonal data, and a requirement for government consultation regarding data transfers. The data localization provisions of the original bill, requiring a copy of any sensitive personal information to be stored in India, remain intact. Although the draft bill in amended form will now [likely be considered during upcoming](#) Lok Sabha parliamentary sessions, India also may [decide to draft new privacy legislation](#) following criticism of the current amended bill by several key stakeholders. In particular, the inclusion of nonpersonal data, the treatment of social media platforms as publishers and the revised structure of the Data Protection Bill have drawn criticism.

South Korea's Adequacy Decision

The European Commission [announced](#) its adoption of an [adequacy decision](#) for South Korea on December 17, 2021, allowing for EU personal data to be freely transferred to South Korea. In its decision, the European Commission [determined](#) that South Korea provides "similar principles, safeguards, individual rights and obligations as the ones under EU law." Additional safeguards were implemented during the adequacy talks to enhance transparency, increase the authority of the South Korean Personal Information Protection Commission (PIPC) and allow PIPC to receive direct complaints from EU data subjects.

Americas

Quebec's Bill 64 – [Bill 64](#) was unanimously adopted last September in Quebec in an effort to modernize Quebec's existing legislation relating to the protection of personal information. Bill 64 is broadly applicable to companies collecting personal information in Quebec, regardless of obligations under other Canadian privacy laws, such as Canada's [Personal Information Protection and Electronic Documents Act](#). Bill 64 introduces data breach reporting obligations, privacy officer appointments, development of organizational privacy frameworks, new individual privacy rights, mandatory privacy impact assessments, and revised transparency and consent requirements. These new requirements will take effect on a rolling basis beginning on September 22, 2022, with the data breach notification and privacy officer appointment obligations. Most of the other new requirements must be implemented by September 22, 2023, but the data portability right does not take effect until 2024. In January, Quebec's DPA, the Commission d'accès à l'information du Québec, [published guidance](#) on the new obligations for businesses and stated that [the business section](#) of its website would continue to be updated with guidance and support tools to assist with Bill 64 compliance.

Uruguay's New Personal Data Transfer Rules for the United States

Last September, Uruguay's DPA, the Unidad Reguladora y de Control de Datos Personales (URCDP), [updated its data transfer regime](#), removing the United States from its list of eligible countries with appropriate privacy protections that could receive personal data from Uruguay. This means that companies previously relying on this justification for transfers of personal data from Uruguay to the United States must now look to other options for their data transfers, including individual consent and contractual clauses ([guidance for drafting contractual clauses](#) was published as well). The URCDP provided a six-month period to make necessary changes to comply, which expires in March 2022. The URCDP also rolled out a new [data breach notification portal](#) in October 2021 and a [personal data protection guide](#) in February 2022.

Update from the Brazilian Data Protection Authority

Brazil's DPA, the Autoridade Nacional de Proteção de Dados (ANPD), [reflected on its first year of work](#) last November, highlighting the completion of the first phase of its regulatory agenda, the publication of new regulations and educational materials, and the receipt of 3,100 requests related to compliance with Brazil's general data protection law, the [Lei Geral de Proteção de Dados](#) (LGPD). With the finalized [enforcement regulation](#) now in place, the ANPD should be able to move forward with its enforcement activities, which include monitoring, education, prevention and sanctions. The ANPD's first monitoring cycle started in January 2022.

Selected Enforcement Actions

The Belgian Autorité de la protection des données–Gegevensbeschermingsautoriteit (APD-GBA) [fined the IAB Europe](#), a digital marketing and advertising association, and [ordered it to amend certain data practices](#) related to its [Transparency and Consent Framework \(TCF\)](#). TCF is a standardized consent solution operated by the IAB Europe that aims to help all parties in the digital advertising ecosystem (for example, publishers and AdTech vendors) comply with the EU GDPR and ePrivacy Directive when processing personal data or accessing and/or storing information on a user's device (for example, cookies, advertising IDs, device IDs). The TCF includes policies and technical standards, including the ability to encode and signal users' privacy preferences in transparency and consent strings (TC Strings). The APD-GBA's decision states that the IAB Europe is a controller of the TCF as a whole. Further, because the TC Strings are personal data under the EU GDPR, the IAB Europe is then a joint controller of a TC String along with other participating entities. This also means that


processing a TC String, even when the purpose of the processing is to indicate no consent, is a type of personal data processing. The IAB Europe [is appealing the APD-GBA's decision](#) to the Belgian Market Court.

In February, the Polish Urząd Ochrony Danych Osobowych (UODO) [fined a utility company](#) just over €1 million for inadequate implementation of appropriate technical and organizational measures, including failure to verify or supervise the processor's security measures. UODO determined that a change made by the data processor resulted in unauthorized copying of and access to a customer database, including by unaffiliated users like the ones that notified UODO of the data breach initially. A smaller fine was ultimately issued to the data processor, which acted inconsistently with common ISO standards and its own data security policy. Separately, the Dutch Autoriteit Persoonsgegevens (AP) issued a [€400,000 fine](#) following a data breach that highlighted the failure of an airline company to maintain complex passwords, multifactor authentication and appropriate account segregation.

Greece's Hellenic Data Protection Authority [fined two telecoms](#) for unlawful retention of records and inadequate security measures following a reported personal data breach. The file in question contained traffic data for subscribers, which was retained for 90 days to assist with resolving problems. After that time, the data was pseudonymized (not anonymized as claimed) and kept for general analytic purposes for 12 months. Information about the retained data was not adequately provided to subscribers. Further, the data protection impact assessment process related to the data retention was incomplete. The company that was actually holding the subscriber traffic data was fined €6 million and ordered to stop its personal data processing and destroy retained personal data. The other company was fined €3.25 million. France's CNIL similarly [issued a €130,000 fine](#) to a payment provider that maintained personal data following a research project in a way that allowed the data to be freely available online for nearly five years. [Excessive retention of personal data](#) was also behind a €2.75 million Dutch AP fine to the Dutch Minister of Finance, which also involved discriminatory practices in relation to the personal data.

South Korea's PIPC continues its active enforcement of national law in a series of fines, including penalties for [incomplete destruction of stored personal data](#), [insufficient data protection measures](#) leading to unauthorized access to personal data, [poor access controls](#) allowing access to the information of other users, and [lack of transparency](#) regarding personal data collection.

Several recent DPA decisions relate to the ability of individuals to exercise their privacy rights under the GDPR. For example, the Österreichische Post [stated in a press release](#) last fall that it had



been fined €9.5 million by the Österreichische Datenschutzbehörde because the newspaper has not been accepting data protection inquiries by email in addition to its web contact form and customer service line. Italy's Garante [fined a telecom €150,000](#) for failing to provide an individual with access to phone records following a prior order to do so, and [fined another two companies €200,000 and €400,000](#) respectively for not allowing individuals to exercise access and objection rights. France's CNIL [fined a mobile telephone](#) provider for not responding to individual rights within the allotted time or appropriately allowing individuals to opt out of marketing communications. The UK ICO [sent the UK's Ministry of Justice](#) a £17.5 million enforcement notice in January for not dealing with its backlog of thousands of incomplete and unanswered data subject requests.

Unwanted marketing communications remain another common reason for regulatory fines. Among the larger recent fines are ones from Italy, Spain and the United Kingdom. Italy's Garante [fined a gas and electric company €26.5 million](#) for "pervasive as well as increasingly invasive" use of unsolicited promotional calls without consent, some of which used prerecorded messages. The company is additionally being asked to implement measures to allow it to manage data subject requests, especially those allowing individuals to opt out of marketing communications. The Garante also [fined a satellite television provider](#) €3.3 million for the subsequent processing of personal data obtained from third-party companies for its own marketing without obtaining new consents or checking the data against its own opt-out lists. Spain's Agencia Española de Protección de Datos (AEPD) [fined an insurance company](#) €300,000 for unwanted marketing communications that continued for several years despite repeated requests to opt out. The ICO [fined a company £140,000](#) for making unconsented pension cold calls, which were previously banned to protect people from those who might try to scam them out of retirement plans.

The Spanish AEPD [fined a financial institution €3 million](#) in relation to its transparency and consent practices in conjunction with offers of credit and other commercial offers. In particular, the AEPD found that the generic information provided did not adequately inform individuals about the distinct types of profiling they may be subject to, and consents for each should have been separately obtained. Cyprus's Commissioner for Personal Data Protection [issued a €925,000 fine](#) for violating transparency obligations to a Wi-Fi surveillance company that was collecting device information during its technology testing without informing the device users. The DPA in Hamburg, Germany, [fined an electric company €900,000](#) for its use of customer data for internal verification purposes related to new-customer bonuses, including comparisons with other customers, without disclosing the use when the personal data was provided.

Several large [identity verification fines](#) have recently been issued by Spain's AEPD. In February, the AEPD [fined several telecoms](#) for not adequately verifying customers' identities prior to issuing SIM cards. This activity led to identity and financial fraud when duplicate SIM cards were provided to unauthorized parties, allowing others [to take over the accounts](#) of authorized users. On the other end of the spectrum, the Dutch AP announced a fine of €525,000 [for disproportionate identity verification](#). This fine to a media company was in response to individual complaints about being required to submit copies of their identity documentation in order for the media company to complete access and deletion requests. The AP found this to be excessive, in particular when the identity documentation needed to be provided via nonsecure communication channels and when the data at issue in the request was not particularly sensitive.

[Shruti Bhutani Arora](#), [Whitney Schneider-White](#) and [Justin Yedor](#) also contributed to the drafting of this Update.

bakerlaw.com

With scores of highly ranked attorneys across multiple practice areas, BakerHostetler helps clients around the world address their most complex and critical business and regulatory issues, delivering sophisticated counsel and outstanding client service. The firm has six core practice groups – Business, Digital Assets and Data Management, Intellectual Property, Labor and Employment, Litigation, and Tax. For more information, visit [bakerlaw.com](#).

Baker & Hostetler LLP publications inform our clients and friends of the firm about recent legal developments. This publication is for informational purposes only and does not constitute an opinion of Baker & Hostetler LLP. Do not rely on this publication without seeking legal counsel.