Report: Nymity - Annual Trending Report - Global

Description: This report displays the top 50 most read References in all countries

Date: March 26, 2019

Date Range: March 26, 2018 to March 25, 2019

1 . GDPR: EU Commission, Parliament and Council Agree to Final Text of General Data Protection Regulation 2016/679 — April 16, 2016

The final text of the GDPR contains 2 levels of penalties for violations of the Regulation; a first level with penalties up to €10 million or up to 2% of the previous year's total worldwide annual turnover (e.g. for violations of the controller's or processor's obligations), and a second level up to €20 million or up to 4% (for violations of the basic processing principles, data subjects' rights, or unlawful international transfers).

2 . Legislation: Brazil Enacts Comprehensive Regime — August 16, 2018

Effective February 15, 2020, controllers must appoint a DPO (to accept complaints and guide employees on data protection), have a legal basis for processing (e.g. consent, legitimate interest, performance of a contract, child's best interest), conduct PIAs (for new products and technologies), comply with data subject requests (portability, correction, consent revocation, review of automated decisions), and notify of security incidents to the DPA and affected data subjects; non-compliance can result in fines up to $13.4 million USD.

3 . Legislation: California Enacts Comprehensive Privacy Rules — July 03, 2018

Effective January 1, 2020, organizations must comply with individual requests to provide categories of personal information collected and shared, stop selling personal information (services cannot be refused and prices cannot be increased as a result), delete personal information, and provide their information in a portable format; the Attorney General can impose civil penalties for violations and there is a private right of action for breaches resulting from reckless behavior.

4 . GDPR: UK Implementing Law Enacted — May 24, 2018

Personal data processing is subject to the GDPR, with the new Act clarifying obligations for legal processing (such as automated processing and special category data), and establishing the age of consent for children at 13; the ICO's powers are expanded to include the issuance of information notices, however, communications protected by client-solicitor privilege are exempt.

5 . Legislation: Polish GDPR-Implementing Law Enacted — May 17, 2018

Current information security administrators can act as DPOs until September 1, 2018, and entities have until July 31, 2018 to notify the DPA of their appointed DPO (where a single DPO acts for a group of entities, each entity must make their own notification), codes of conduct must be submitted to the DPA for approval (compliance will be monitored), and administrative proceedings currently underway under the current *Data Protection Act* will continue to have effect.

6 . Legislation: Austria Amendments Implementing the GDPR — July 14, 2017

New grounds for processing include explicit legal authorisation or a controller's legitimate interests for criminal data (under court or administrative authority), and minors' consent for processing by information society services (if age 14 and over); images are now included in the scope of personal data and may be processed with consent, for protection of private property, or for surveillance of public areas, and companies can now be held liable for data protection violations (in addition to current provisions for natural persons).

7 . Legislation: Most Countries Have a Data Privacy Law — April 13, 2018

Of the 24 countries surveyed by this advocacy group, only Brazil and Thailand do not have data protection laws; other findings indicate that only Australia, Canada, Korea, Mexico, South Africa and U.S. have breach notification laws.

8 . Legislation: Colorado Amends Breach and Destruction Laws — June 04, 2018

Effective September 1, 2018, companies have to implement reasonable security (risk assessment required) and disposal policies and procedures (shredding, erasing), notify individuals of breaches within 30 days from the date of the breach (including cases where the confidential process or encryption key was also acquired), and report breaches to the State AG (within 30 days) if more than 500 residents are affected.

9 . GDPR: Italy Enacts Implementing Decree — September 18, 2018

The Decree amends the current *Privacy Code* to integrate the provisions of the GDPR; organisations should appoint a person in charge of monitoring compliance within each department, biometric data may only be used for purposes of physical security and access procedures, and only consent can be used for marketing purposes (rather than legitimate interest as permitted under the GDPR).

10 . GDPR: Dutch Implementing Act Enacted — May 25, 2018

The current *Personal Data Protection Act* is withdrawn; personal data processing is subject to the GDPR, with the new Act establishing the age of consent at 16, outlining processing requirements for special category data and national IDs, not requiring individual breach notification for financial companies subject to the *Act on Financial Supervision*, obliging DPOs to keep complaints and requests received confidential, and conducting legal proceedings prior to May 25, 2018 under the current Act.

11 . GDPR: Greece Proposed New Data Protection Act — April 17, 2018

The legislation sets children's consent for information services at age 15, requires prior DPA consultation for large-scale processing of creditworthiness data, prohibits genetic screening for health/life insurance purposes, permits employee monitoring subject to certain conditions (but grants them the right to complain to the DPO), penalizes a DPO who violates their professional secrecy obligations, and permits an aggrieved data subject to file a claim for damages.

12 . GDPR: German State DPA Publishes List of Mandatory DPIAs — August 16, 2018

Such processing includes vehicle data using automatic readers, merging of data using non-transparent algorithms (e.g., fraud prevention), behavioural/performance evaluation assessments (e.g., ratings portals, collection services, geolocation of employees), online profiling (e.g., dating sites and social networks), Big Data, artificial intelligence, location tracking (e.g., in shopping malls), RFID (e.g., by apps/maps), and centralized storage of measurement data (e.g., fitness apps).

13 . Legislation: Indian Government Task Force Issues GDPR-Like Bill — August 02, 2018

The Bill, if enacted, would impose obligations on controllers (including notice, collection/purpose limitations, and data localization), require certain organisations to conduct DPIAs, data audits and notify breaches to a newly-created DPA, potentially apply to foreign processors, and impose consent and adequacy requirements on cross border transfer flows; non-compliance would be punishable by fines of up to 4% of total worldwide turnover.

14 . GDPR: Denmark Enacts Supplementary Law — June 15, 2018

The Law requires prior DPA authorisation for determinations of creditworthiness, prescribes explicit restrictions on debt transmission, direct marketing and selling of marketing lists, sets children's consent at age 13, and governs CCTV and the processing of decedents' data for 10 years; DPA powers are enhanced (able to restrict international data transfers where no adequacy decision applies), and criminal liability may apply to companies for statutory violations.

15 . GDPR: France Enacts Implementing Amendments — July 03, 2018

Amendments include the obligations to obtain joint consent from the data subject and a parent or legal guardian for processing digital data of children under the age of 15, and prove that customer contracts regarding online publications do not prevent the user from providing valid consent; periodic penalties have been added, with amounts not exceeding €100,000 per day's delay.

16 . GDPR: Irish Implementing Law Enacted — May 28, 2018

The current Data Protection Act is amended to incorporate GDPR requirements; the age of consent is set at 16 years, processing is permitted for special category data (e.g., insurance and pension purposes, legal claims and proceedings, medical diagnosis), data subjects rights can be restricted to safeguard public interest, fees may be charged for cross-border transfer approvals, and fines for data protection violations

cannot be imposed on entities already subject to criminal penalties.

17 . Legislation: Belgian Law Solidifies DPA Powers January 18, 2018

Effective May 25, 2018, the DPA will replace the Commission for the Protection of Privacy ("Commission"), with powers to conduct on-site inspections, access personal data held by organisations and issue warnings, and issue administrative fines and data processing suspensions; complaint proceedings initiated prior to the effective date of the Act will continue, but will be subject to the powers previously held by the Commission.

18 . GDPR: Italy Drafts Supplemental Decree May 08, 2018

If passed, general authorizations and previous DPA decisions/order will remain effective where compatible with the GDPR, biometric data can only be processed through provisions determined by the DPA, and location data can only be processed if anonymous or with express consent; parental consent is required on behalf of children under 14, and lying to the DPA or disrupting an investigation is subject to imprisonment from 6 months to 3 years.

19 . GDPR: Polish DPA Final List of Mandatory DPIAs September 10, 2018

New processing activities included in the list include profiling to incentivise use of services and analysis of data collected from other sources to create profiles (shopping history, banking operations, website history); activities removed from the list include processing of medical records, cross border transfers, and customer check systems in credit information databases.

20 . GDPR: Spain Enacts Implementing Law December 12, 2018

Effective December 7, 2018, the age of consent is set at 14 years, the DPA must be notified of appointed DPOs within 10 days (even for voluntary appointments), consent cannot be used to identify special categories of data, and search engines and social networks must comply with removal requests where data is inaccurate, inadequate, irrelevant, outdated, excessive or no longer in the public interest.

21 . Legislation: Croatia Enacts GDPR-Implementing Law May 14, 2018

Limitations are imposed on processing of biometric data (only where legally required, for protection of life, property, classified information, or for customer ID), genetic data (consent required for life insurance contracts, calculations of illness, or health issues), and video surveillance (only if necessary for protection of persons or property, or in accordance with occupational safety regulations). Fees will be charged for DPA opinions, and current administrative proceedings will continue under the current *Data Protection Law*.

22 . Data Localization: Vietnam Imposes Obligations June 06, 2018

A Decree on internet services requires social networks, aggregated information websites, mobile telecoms and online game services to maintain at least 1 server in Vietnam and store all user registration information and posting history; a draft cybersecurity law would require telecoms and ISPs to maintain all citizens' PI on servers located in Vietnam.

23 . GDPR: Implementing Law Enacted in Hungary July 27, 2018

The law applies to manual data processing (even if not contained in a filing system), creates an age of consent for online services of 16 years, requires a Parliamentary act or municipal decree for processing based on compliance with a legal obligation or performance of a public interest task, no longer requires registration of processing (however archived information will be used for investigations before May 25), and provides individuals with a private right of action for violations.

24 . Data Subjects Rights: Differences Between the GDPR and CCPA October 16, 2018

Businesses caught in the scope of both laws will have to implement separate measures to comply with consumer requests; the GDPR requires more information be provided in access requests (retention periods, automated decision making), businesses must transfer users' personal data to another business (the CCPA only requires provision to consumers in a useable electronic format), and individuals have much broader rights to restrict or object to processing (not just sale of their data).

25 . GDPR: Slovakia Enacts Data Protection Law January 04, 2018

Effective measures must be in place to ensure that inaccurate personal data is erased or corrected

without undue delay, and provisions that have been removed from the draft include the applicability of the Law to deceased individuals and the guarantee of personal data transfers to EU Member States.

26 . GDPR: Sweden Enacts Complementary Law June 07, 2018

The provisions do not apply to processing for the purposes of journalism, academia or artistic or literary creation, parental consent is required for processing of children under the age of 13, and notice requirements do not apply to any data that the controller is legally restricted from disclosing.

27 . Best Practices: OPC and OIPC Guide Companies on Consent August 17, 2018

To obtain express and informed consent, companies must involve users when designing the consent process and conduct regular audits of privacy communications to ensure they reflect management policies; mobile apps guidance recommends limiting data to that which is needed by the app to function and providing a dashboard for users to easily tighten privacy settings.

28 . Legislation: South Dakota Enacts Breach Notification March 26, 2018

Unauthorized acquisition of computerized data (including any encryption keys) compromising the security, confidentiality or integrity of personal or online account information must be reported to affected State residents (within 60 days), the AG (if more than 250 residents are affected), and CRAs (without undue delay); entities will be in deemed compliance if notification is in accordance with federally-regulated breach procedures (e.g., HIPAA and GLBA).

29 . Legislation: Brazilian Senate Approves Comprehensive Regime July 25, 2018

Data controllers must appoint a DPO (to accept complaints and guide employees on data protection), have a legal basis for processing (e.g. consent, legitimate interest, performance of a contract, child's best interest), conduct PIAs (for new products and technologies), comply with data subject requests (portability, correction, consent revocation, review of automated decisions), and notify of security incidents to the DPA and affected data subjects; non-compliance can result in fines up to $13.4 million USD.

30 . Legislation: Arizona Amends Breach Notification Law April 19, 2018

Effective August 3, 2018, companies must report breaches involving biometric data, private authentication keys, SSNs, health insurance IDs, passport number, taxpayer IDs, and username or email addresses (with passwords or security questions and answers); notification must be provided to affected individuals within 45 days, and if more than 1000 individuals are affected, the AG and the 3 major CRAs must also receive notification.

31 . Legislation: Austria Amends its GDPR-Implementing Law May 09, 2018

The amendments clarify that the fundamental right to privacy applies to natural persons only, and prohibit combining CCTV images with other personal data to create personal profiles. Provisions allowing non-profits to seek compensation on behalf of individuals for privacy violations have been removed, and offences levied under the previous data protection law can now be appealed on the basis that the new law provides a more favorable legal position.

32 . GDPR: Bulgaria Introduces Implementing Bill May 03, 2018

DPO appointment is required where entities process more than 10,000 individuals' personal data (internal or external appointment is permitted), the age of consent is set at 14 years, employers can copy employee identity cards, drivers licenses, travel documents and residence information, can process employee data based on explicit consent (where processing is not legally required), and can retain job applicants' personal data for up to 3 years.

33 . GDPR: ICO UK Details High Risk Processing June 01, 2018

Personal data processing requiring DPIAs - intelligent transport systems, dating websites, market research involving neuro-measurement, contract pre-check processes, social media networks, list brokering, wealth profiling, re-use of publicly available data, and eye tracking; consider risks to individual rights and freedoms (inability to access services or exercise rights, identity theft or fraud), and identify mitigating measures (reducing retention periods or processing scope, anonymisation, human review of automated decisions).

34 . Legislation: California's Consumer Privacy Bill Raises Concerns June 18, 2018

A law firm discusses how the broad scope of the *California Consumer Privacy Act* ("CCPA") to protect the information of any California resident means financial institutions would be subject to it various privacy obligations with respect to its customers, employees and vendors who reside in the state; the CCPA does not have any practical exceptions to a consumer's right to opt-out of the sale of their PI to facilitate disclosures made in the regular course of business (e.g., to an affiliate).

35 . Legislation: California Bill Delays CCPA Enforcement August 29, 2018

If passed, the AG cannot bring enforcement actions until the earlier of July 1, 2020 or 6 months after regulations are issued, new exceptions to compliance with the Act's rights and obligations include infringement on a business' non-commercial activities, clinical trial information, and personal information collected under the *Financial Right to Privacy Act*, and penalties can be imposed up to $2,500 for each violation (or up to $7,500 for intentional violations).

36 . Transparency: Impact of California's Consumer Privacy Act July 30, 2018

A law firm notes that Canadian organizations may be subject to the Act if they offer products or services to California residents; two or more methods must be in place for these individuals to make access, deletion, opt-out and data portability requests, a conspicuous website link must be provided for consumers to opt-out of sale of their PI, and enforcement can include private rights of action for security breaches and AG civil penalties.

37 . Legislation: Spain Proposes Draft Data Protection Bill Enacting the GDPR July 12, 2017

If passed, the processing of sensitive data will be prohibited, regardless of whether or not the data subject consents to the process (alternative grounds for processing sensitive data will be provided in a separate law that will address additional security measures); organisations have a duty to cooperate with the DPA when requested as part of a DPA investigation into the organization's clients.

38 . Legislation: Oregon Amends Breach Requirements March 19, 2018

Entities must notify affected individuals of a breach involving their personal information (which now includes any combination of information permitting access to a financial account) within 45 days of discovery or notification, and provide the AG with a copy of the notice. CRAs are prohibited from conditioning provision of credit monitoring or identity theft protection services on acceptance of other services, or consumer provision of their debit or credit card.

39 . GDPR: Luxembourg Enacts Law August 22, 2018

The Law exempts processing for journalistic, academic, literary or artistic purposes from certain obligations under the GDPR, imposes measures on processing scientific, historical research or statistical purposes (including appointment of a DPO, a DPIA and anonymisation/pseudonymisation), and permits surveillance subject to certain conditions; obstruction of any of the DPA's tasks is punishable by imprisonment and/or a fine.

40 . GDPR: Belgium Enacts Supplementary Law September 07, 2018

The processing of health-related, biometric and genetic data is permitted where additional security measures are taken (e.g., controlled access to the data and confidentiality obligations), parental consent is required for processing personal data of children under the age of 13, and restrictions exist on data subject rights when processing involves journalistic, academic, artistic or literary expression.

41 . Legislation: Similarities Between Brazil's New Law and the GDPR November 05, 2018

Like the GDPR, Brazil's law applies extraterritoriality to personal data processing that offers goods or services to individuals in Brazil (regardless of controller location), requires DPO appointments, and provides data subjects rights of access, portability, erasure, consent revocation, and review of automated decisions; however, breach notification to data subjects and the DPA is required for any incident that may result in risk or damage (not just those with a high risk).

42 . GDPR: France Amends Draft Law February 26, 2018

Parental consent is required for processing the personal data of minors under the age of 15 for information society services, and controllers must make information aimed at minors easily accessible,

and present it in clear language; controllers must inform individuals the main characteristics of automated processing upon request, with the exception of any processing secrets protected by law.

43 . Employee Privacy: AP Region Transparency and Transfer Requirements April 05, 2018

Employers must develop a separate data privacy policy for employees in Hong Kong, Indonesia, Singapore and South Korea; while there is no express requirement, it is recommended to develop policies in China, Japan, and Thailand. Overseas transfers are unrestricted in Thailand, however, all other countries restrict transfers (by requiring consent, or ensuring the recipient maintains adequate protection).

44 . Employee Privacy: AP Region Consent Requirements April 02, 2018

Employers must obtain consent for processing employee data in China, Hong Kong, Japan, Singapore, and South Korea (prior notification of the purposes of collection is required), however there are no express consent requirements in Indonesia, or Thailand (however, consent should be obtained to avoid privacy rights claims).

45 . GDPR: Norway Enacts Personal Data Act July 13, 2018

Effective July 20, 2018, parental consent for information society services is required for children under 13, special category data may be processed without consent for archival, scientific, historical or statistical purposes in the public interest (if it does not disadvantage the data subject), and exemptions to the rights of notice and access include detriment to health and obligations of secrecy.

46 . GDPR: France Enacts Supplemental Decree August 28, 2018

Areas addressed include - data subjects rights may be limited in certain aspects of processing scientific or historical research and statistical data, encryption must be used when transmitting health data, data controllers have 2 months to respond to an access request, and breach notification is not required where a person's anonymity is protected under legislation regarding freedom of the press.

47 . Legislation: Canada's Breach Notification Regulations April 20, 2018

Effective November 1, 2018, organizations must report a breach of security safeguards in writing to the federal Commissioner, which includes circumstances and cause (if known) of the breach, the PI subject to the breach, and steps taken to mitigate risks and notify individuals; notification must be made to affected individuals in person, or by telephone, mail or email.

48 . GDPR: DPA Belgium Final DPIA Guidance April 13, 2018

A DPIA is not required for processing focused on payroll, administrative employee data, accounting data, and most processing by schools and non-profits; where a DPIA is not conducted, despite meeting the criteria for one, the reason must be approved by the DPO and documented.

49 . GDPR: CNIL Recommendations for Valid Consent September 04, 2018

Individuals must have a real choice in processing of their personal data (consent cannot be influenced by negative consequences of refusal), provide separate consents for each single processing purpose (purposes should be explicitly differentiated), and be provided with proper notice (i.e. purposes, categories of data, right of withdrawal).

50 . GDPR: Romania Enacts Implementing Law August 01, 2018

The law permits processing of genetic, biometric or health data (pursuant to express consent and protective measures), and monitoring of employee electronic communications or via video surveillance for an employer's justified legitimate interests (subject to prior notice to employees and their representatives, the inability to use less intrusive methods, and retention for no more than 30 days).

Important Legal Notice

This Report may only be redistributed within your organization, provided that Nymity trademarks, logos and this copyright notice are not removed. This Report may not be sold for profit or used in commercial documents without the written permission of Nymity.

The content of the Report is provided "as is" without any express or implied warranty. The Report does not constitute legal advice and no attorney-client relationship is formed between any subscriber or recipient and Nymity. If you require legal advice, you should consult with an attorney. Use of the Report and its content are subject to the Terms of Use and Disclaimers available at https://www.nymity.com/legal-notices.aspx.