Fourth Annual Latin America Privacy & Cybersecurity Symposium

KPMG FORTINET OneTrust Privacy Management Software ICC MEXICO INTERNATIONAL CHAMBER OF COMMERCE The world business organization iapp EGADE Business School Tecnológico de Monterrey JONES DAY

GLOBAL OUTLOOK: THE GDPR, CALIFORNIA AND BRAZIL'S DATA PROTECTION ACTS, AND OTHER GLOBAL TRENDS

Presented by

Richard Martinez, Jones Day
Olivier Haas, Jones Day
Jose Antonio Batista de Moura Ziebarth, Brazil's Ministry of Economy
Diego Gualda, Machado Mayer
Rocky Tse, OneTrust

JONES DAY

GLOBAL OUTLOOK ON PRIVACY TRENDS

Key Trends after One Year of GDPR

Presented by

Olivier Haas
Partner – Jones Day
ohaas@jonesday.com

JONES DAY

AGENDA

1. The GDPR: Facts and Figures after 1 Year
2. Guidance on GDPR: Clarifications Available and Outstanding Issues
3. Current Priorities for Implementing GDPR Compliance
4. Key Points for Maintaining Compliance
5. The GDPR: a global standard?

JONES DAY

1- THE GDPR: FACTS AND FIGURES AFTER 1 YEAR

- GDPR: a Game Changer for data protection in the EU with a global impact
  - A strongly unified regulatory framework for data protection including cooperation and consistency mechanisms between supervisory authorities
  - A major shift from prior formalities to accountability, with a global impact
  - Increased obligations for controllers/processors: information/consent, documentation, security, subcontracting, data breach notification/communication
- GDPR enforcement is ramping up
  - Over 200,000 national cases, ~70,000 data breach notifications
  - Larger fines ranging from EUR 150k to 50M – total aggregated fines ~EUR 56M
  - Main topics: information, legal bases/consent, security

JONES DAY

2- GUIDANCE ON GDPR - CLARIFICATIONS AVAILABLE AND OUTSTANDING ISSUES

- The GDPR is a fairly detailed regulation: Is that enough?
- WP29 and the European Data Protection Board have issued important guidance on key issues – over 20 guidelines/position papers already:
  - Territorial Scope of the GDPR
  - Transparency / Consent / Processing for performance of online services
  - Automated decision-making and Profiling
  - Data Breach notification
- Upcoming guidance from the EDPB:
  - Controller/processor, Data Subject Rights, Targeting, Videosurveillance etc.
  - Interplay with other regulations: e.g. PSD2

JONES DAY

3- CURRENT PRIORITIES FOR IMPLEMENTING COMPLIANCE

- Most businesses have addressed
  - Public facing side of GDPR compliance: Privacy policies and notices
  - Internal documentation items: Record of activities, policies and procedures (*e.g.* security), data transfer agreements, training material
- But the compliance effort is not over yet
  - Privacy Impact Assessments need to be carried out and formalized
  - An Incident Response Procedure must be implemented
  - Documentation and procedures need to be further developed:

    e.g. Data protection by design and by default, Procedures to respond to Data Subjects' Requests

JONES DAY

4- KEY POINTS FOR MAINTAINING COMPLIANCE

- And then: *Finally done?... Well, not quite yet I'm afraid!*
- Compliance needs to be maintained:
  - Revise and refine the GDPR compliance setup in light of available guidance
  - Ensure the policies and procedures are applied
  - Implement internal audits
  - Review compliance of / audit vendors & data processors

JONES DAY

5- THE GDPR: A GLOBAL STANDARD?

- The territorial reach of the GDPR extends well beyond the EU because of:
  - The actual territorial scope of the regulation
  - The need of global businesses to standardize their setup for processing personal data
  - The many new regulations that are being adopted and implement GDPR-like principles
- Lessons being learned from the GDPR compliance effort will be most useful to adjust to the various new international data protection regulations

JONES DAY

THE CALIFORNIA CONSUMER PRIVACY ACT (CCPA)

Presented by

Richard Martinez
Partner – Jones Day

rmartinez@jonesday.com

JONES DAY

OVERVIEW: WHAT IS THE CCPA?

- Signed into law on June 28, 2018 by Governor Brown.
- Represents the latest change to California privacy law and toughest privacy law in the U.S.
- Creates statutory damages for data breaches.
- Grants consumers more control over and insight into the spread of their personal information online.
- Imposes on businesses additional obligations related to notice, disclosure, and response to consumer requests.
- Set to enter into force January 2020.

BRIEF COMPARISON WITH THE GDPR

- The CCPA shares similar general features with the GDPR but differs in scope.
- Compliance with GDPR will not be sufficient to meet CCPA requirements.

Topic	GDPR	CCPA
Whose data is protected?	Natural person in the EU	California consumers (i.e., residents)
Scope	Omnibus law on wide range of topics including notice, legal basis, cross-border data transfers, data breach notification, etc.	Focuses primarily on consumer rights and disclosures required to consumers.
Individual Rights	Access, deletion, rectification, objection, data portability, not to be subject to automated decision making, etc.	Access, opt-out, deletion, equal services

SCOPE OF THE CCPA

WHO IS COVERED?

- **"Consumers"** – natural persons who are California residents.
- **"Businesses"** – Legal for-profit entities that do business in California and meet one of the following:

1. Have annual gross revenues over $25,000,000
2. Hold the personal information of 50,000 or more consumers, households, or devices
3. Derive at least 50% of annual revenues from selling consumers' personal information.

SCOPE OF THE CCPA

WHAT DATA?

- **"Personal Information"** – Information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.

WHO IS NOT COVERED?

- Not-for-profit organizations
- State or local government entities
- Small businesses that do not traffic large amounts of personal information from California residents
- Companies that do not share a brand with affiliates covered by the CCPA
- Narrow exception for commercial conduct wholly outside California that meets following criteria:

1. The business collected the information from the consumer in question while he or she was outside California,
2. No part of any sale of his or her personal information occurred in California, and
3. No personal information collected while the consumer was in California is sold

THE GRAMM-LEACH-BLILEY ACT/CALIFORNIA FINANCIAL INFORMATION PRIVACY ACT EXEMPTION

- Financial institutions and other entities regulated by the GLBA and California Financial Information Privacy Act ("CFIPA") will still be impacted
  - **The CCPA applies to data that falls outside the scope of these statutes**
    - The CCPA definition of personal information is broader than the GLBA and CFIPA definitions of "nonpublic personal information" because the CCPA is not limited to information regarding financial products or services.
    - Thus, if financial institutions collect information that is covered by the CCPA but not the GLBA/CFIPA, then the exemption may not provide much protection.
      - E.g., tracking website visitors, targeted online advertising, business contacts.
    - How financial institutions distinguish the types of data exempt and covered by the CCPA remains to be seen; may see additional, clarifying CCPA amendments
  - **Data governed by these statutes is still subject to private rights of action in the event of a data breach**

NEW RIGHTS AND LIABILITIES

CALIFORNIA RESIDENTS' NEW RIGHTS

- Right to Notice
- Right of Access
- Right to Data Portability
- Right to be Forgotten
- Right to Opt Out of Information Sales
- Right to Non-Discrimination

JONES DAY

RIGHT TO NOTICE

Businesses must **notify** consumers via online privacy policies or at or prior to time of collection of:

- Categories of personal information collected
- Purposes for which personal information is used
- Specific pieces of information collected
- A description of consumers rights and how to exercise them
- Categories of personal information collected within past 12 months, if any
- Categories of personal information sold or disclosed within past 12 months, if any

- Online privacy policies / websites must be updated annually.

RIGHT OF ACCESS

- Consumers may request disclosure of specific information from businesses:
  - Categories of personal information collected
  - Categories of sources from which business collected personal information
  - Purposes for collecting or selling personal information
  - Specific **"*pieces* of personal information"** that a business has collected (i.e., a copy of the personal information about the consumer)
  - Third-party recipients with whom personal information was shared or sold
- Significantly expands upon California's existing Shine the Light Law and Online Privacy Protection Act.

RIGHT TO DELETION ("RIGHT TO BE FORGOTTEN")

- Businesses – and their service providers – must comply with consumer requests to delete their personal information, ***unless*** the data is necessary to:
  - Complete a transaction, provide a good or service requested by the consumer, or perform a contract between the business and the consumer
  - Detect security incident or other malicious or fraudulent activity
  - Debug to identify and repair errors
  - Exercise free speech
  - Comply with the CA Electronic Communications Privacy Act or other legal obligations
  - Engage in scientific, historical or statistical research in public interest
  - Enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business
  - Be used internally in a lawful manner that is compatible for the purpose for which it was provided

RIGHT TO OPT OUT AND OPT IN (FOR MINORS)

- Consumers can **opt-out** of the sale of their personal data to third parties.
- Businesses must post a clear and conspicuous link entitled **"Do Not Sell My Personal Information"** on their national website or California-specific webpage directing users how to opt-out of the sale of their personal data.
- Businesses must wait 12 months before requesting consumers who have opted out to authorize the sale of their personal information.
- **Opt-In for Minors:** Businesses must obtain permission of consumers between ages 13-16 and parental consent from minors age 13 or less prior to selling their personal information.

RIGHT TO NON-DISCRIMINATION

- A business cannot discriminate, or suggest it will discriminate, based on an exercise of CCPA rights by:
  - Denying goods or services
  - Providing different level of goods or services
  - Charging different prices or rates
- But a business can charge different prices or offer different levels of service if it is “reasonably related to the value provided the consumer by the consumer’s data.”
- And a business can offer certain incentives to allow the business to collect, sell, or not delete data.

PRIVATE RIGHT OF ACTION:
LIABILITY FOR DATA BREACHES

- Businesses have duty to implement and maintain ***reasonable security procedures*** and practices appropriate to the nature of the information to protect the personal information.
- Consumers have **private right of action** – on individual or class-wide basis – when their non-encrypted or non-redacted personal information is subject to data breach as a result of the business' violation of its duty.
- Consumers can
  - Recover damages between $100 - $750 per incident or actual damages, or
  - Seek injunctive or declaratory relief
- For breach liability, definition of personal information follows California state data breach notification law
  - Individual name + SSN, driver's license/ID number, account number, credit or debit card number, username and password, medical information, or health insurance information

OPERATIONAL IMPACTS

- Many companies, even those outside the U.S., will be subject to the CCPA
- Increased cost for compliance associated with updating online privacy policies, individual rights policies and procedures
- Increased consumer-driven litigation for data breaches
- In addition to exposure to consumer-driven litigation, exposure to litigation and fines for actions by California Attorney General
- Additional burdens placed on network security personnel to protect the network while justifying retention of “personal information”

THE ROAD AHEAD:
10 STEPS TO IMPLEMENTATION

- Monitor and map data intake/sharing/selling practices in order to timely respond to data disclosure requests
- Evaluate reasonableness of data security measures employed to protect personal information
- Determine whether the CCPA applies to any part of the business
- Conduct a gap analysis to assess current practices and procedures versus CCPA requirements
- Assess risk level, risk appetite and all relevant insurance coverage

THE ROAD AHEAD:
10 STEPS TO IMPLEMENTATION

- Develop consumer rights policies and implement mechanisms to effectively and timely respond to consumers
- Revise and annually update online privacy policies to include required informational notices and disclosures
- Develop and monitor mechanism to manage request to opt-out of sale of personal information
- Determine age of California residents and obtain consumer and/or parental consent for sharing of minor's personal data

THE ROAD AHEAD:
10 STEPS TO IMPLEMENTATION

- Provide clear and conspicuous “Do Not Sell My Personal Information” link on the internet home page for consumers opt out of sale of personal information
- Review and update contracts with vendors and other service providers for compliance with CCPA

POTENTIAL LEGISLATIVE EFFORTS

➔ Amend the CCPA

➔ Prevent patchwork of state privacy laws

➔ Pass federal law preempting state privacy laws

JONES DAY

RULEMAKING AND LITIGATION EFFORTS

- California AG's Rule-Making
- Litigation Challenges

DATA PROTECTION IN BRAZIL ON A POST GDPR ERA

What to know about Brazilian Personal Data Protection Law

Law n. 13.709/2018 (“LGPD”)

Presented by

Diego de Lima Gualda
dlgualda@machadomeyer.com.br

AGENDA

- What we know
- What we do not know
- What to do

WHAT WE KNOW

- Data Protection will continue to be a topic of debate, transformation and changing for all different players on a global scale
- LGPD is highly inspired in GDPR, following the main E.U. legislation features
- Yet, there are some important differences, including the fact that LGPD has plenty of open concepts (with no recitals nor previous institutional background)
- Data protection is relatively new in Brazil, for companies and for the authorities

WHAT WE DO NOT KNOW

- How successful post GDPR legislation will be, especially on the promise of regain control to data subjects
- Brazilian legal certainty issues are aggravated by the unfinished legislative process and the lack of formed Data Protection Authority
- How main concepts of the law will be interpreted

WHAT TO DO

- **Do for sure:** information security measures; training your people; know your business; and be accountable
- **Do…, but carefully:** pay attention to trade-offs; be careful to not compromise the future of your business; consider to take some calculated risks
- **Do not forget to consider:** no company is an island, engage with your stakeholders

Jones Day presentations should not be considered or construed as legal advice on any individual matter or circumstance. The contents of this document are intended for general information purposes only and may not be quoted or referred to in any other presentation, publication or proceeding without the prior written consent of Jones Day, which may be given or withheld at Jones Day's discretion. The distribution of this presentation or its content is not intended to create, and receipt of it does not constitute, an attorney-client relationship. The views set forth herein are the personal views of the authors and do not necessarily reflect those of Jones Day.