Arnold & Porter

Privacy in 2019: Two-Part Session
Post-GDPR Roundtables and California Consumer Privacy Act Boot Camp

Michael Kallens, *Nasdaq*
Rob Bratby, *Arnold & Porter*
Nancy L. Perkins, *Arnold & Porter*

March 20, 2019

Contact Information

Michael Kallens
Sr. Associate General Counsel
Michael.Kallens@nasdaq.com
+1 301.978.8423

Rob Bratby
rob.bratby@arnoldporter.com
+44 77 3831 2629

Nancy L. Perkins
nancy.perkins@arnoldporter.com
+1 202. 942.5065

Session #1: Post-GDPR Roundtables

Business Challenges (Topics for Table Discussions)

1. To whom does the GDPR apply (territorial scope)?
2. What privacy issues arise when personal data leaves the EU?
3. How should data subject access requests be dealt with?
4. How should you prepare to respond to a data security breach?

Topic #1:
Does the GDPR apply to me?

Art. 3 GDPR - Territorial Scope

The GDPR applies to:

1. the processing of personal data in the context of the activities of an establishment of a controller or a processor in the EU, regardless of whether the processing takes place in the EU or not.
2. the processing of personal data of data subjects who are in the EU by a controller or processor not established in the EU, where the processing activities are related to:

   (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the EU; or

   (b) the monitoring of their behaviour as far as their behaviour takes place within the EU.
3. the processing of personal data by a controller not established in the EU, but in a place where Member State law applies by virtue of public international law.

Does the GDPR Apply?

Step 1: – personal data

- GDPR applies to any information **relating to an identified or identifiable [living] natural person** – so **not to anonymised data**
- **Pseudonymised** (e.g. key-coded data) is expressly still caught

Step 2: – in or targeting individuals in the EU

1) **Are you established in the EU and processing personal data in the context of that establishment?**
   - office / employees / branch?
2) **Are you offering goods / services to EU individuals? (Even if ex-EU)**
   - offering products to order or related services remotely / on your website
   - directing sales and marketing activities to EU individuals
3) **Are you monitoring the behaviour of EU individuals? (Even if ex-EU)**
   - online tracking and profiling

→ EU guidance on territorial scope "in progress"

How are you characterized under the GDPR?

Key issue = are you a controller or a processor?

Distinction

- **Controllers** determine purposes and means of any personal data processing
- **Processors** process personal data on behalf of controllers

→ no new guidance on controller v processor under GDPR, but definitions have not materially changed since previous legislation

→ GDPR expressly provides for joint control (*Art 26 GDPR*) – replaces old (non-statutory) concept of "controllers in common"

  - Requires an arrangement (although not necessarily a written agreement) setting out each joint controller's responsibilities for GDPR compliance
  - Regardless of the terms of this arrangement, data subjects may exercise their rights against each controller

Case Law on Controller/Processor Distinction

Recent CJEU case law

C-210/16 Wirtschaftsakademie Schleswig-Holstein - data processed via cookies on devices of fan page visitors, to provide data to Facebook and fan page admin

- Fan page administrator was a joint controller with Facebook:
  - By creating the page, gave Facebook the opportunity to place cookies
  - Used filters to define stats collected by Facebook, e.g. age, sex, lifestyle, location
  - Therefore "took part" in the determination of purposes and means of processing
  - Even though it only received anonymised data from Facebook

C-25/17 Jehovan todistajat - data processed via preaching by members of the Jehovah's Witnesses Community – name, address, religious beliefs

- Jehovah's Witness Community was a joint controller with individual members:
  - Although individual members determined specific data collected, the community "exerts influence" over that processing, and organises, coordinates and encourages the preaching
  - Didn't matter that community had no access at all to the data concerned

Controller and Processor Obligations

Controllers

- **have the main obligation for GDPR compliance, which includes record keeping and adhering to GDPR 'principles', including:**
  - data processed lawfully, fairly and transparently (e.g. by a privacy policy)
  - data is adequate, relevant, necessary, accurate, and is processed securely

Processors

- **now have obligations under GDPR as well as controllers:**
  - technical – privacy by design and default
  - governance - record keeping
  - notification – to controller without undue delay after aware of data breach
  - potential high fines also (in addition to relevant controller's fines)

- Written contract needed between controllers and their processors setting out specific obligations that the processors must adhere to

Topic #2:
How do I export personal data from EU?

Art. 44 GDPR - General Principle for Transfers

Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country shall take place only if the GDPR data-protection conditions are complied with by the controller and processor, including for onward transfers of personal data from the third country to another third country.

- Art 45 – Transfers on basis of adequacy decision (i.e. Privacy Shield)
- Art 46 – Transfers subject to appropriate safeguards (i.e. model clauses)
- Art 47 – Binding corporate rules
- Art 48 – [Transfers pursuant to international treaty obligations]
- Art 49 – Derogations for specific situations (n.b. very limited scope for use of consent)

How to Comply: International Transfers of Data (1)

- General prohibition on transferring personal data out of EEA
- Consider if there has been an 'adequacy decision' by EU Commission (Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay, US (limited to the Privacy Shield framework)
- Otherwise, must ensure destination provides 'appropriate safeguards' for such transferred personal data (so similar to requirements under current legislation)
- There are derogations however (*Article 49 GDPR*) – including a finely balanced "compelling legitimate interests pursued by the controller"
- In a potential litigation context, consider if Article 49(9)(e) applies:

  "*the transfer is necessary for the establishment, exercise or defence of legal claims*"

How to Comply: International Transfers of Data (2)

- Consent **may** be possible / relevant, but consider other such appropriate safeguards:

1) **Standard contractual clauses** (in a Data Transfer Agreement (DTA))
2) **Privacy Shield**
   - EU-US and Swiss-US (so only relevant to US based organisations)
   - organisations self-certify to US Department of Commerce and adhere to Privacy Shield requirements (which are similar to the GDPR)
3) **Binding Corporate Rules (BCRs)**

Both subject to pending legal challenges, and US compliance with Privacy Shield under scrutiny by MEPs

Topic #3:
Data subject access requests

Art. 15 GDPR- Right of access by the data subject

1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:
   (a) the purposes of the processing;
   (b) the categories of personal data concerned;
   (c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
   (d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
   (e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
   (f) the right to lodge a complaint with a supervisory authority;
   (g) where the personal data are not collected from the data subject, any available information as to their source;
   (h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.
3. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.
4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

Sample Compliance Checklists (Source: ICO)

Preparing for subject access requests

- We know how to recognise a subject access request and we understand when the right of access applies.
- We have a policy for how to record requests we receive verbally.
- We understand when we can refuse a request and are aware of the information we need to provide to individuals when we do so.
- We understand the nature of the supplementary information we need to provide in response to a subject access request.

Complying with subject access requests

- We have processes in place to ensure that we respond to a subject access request without undue delay and within one month of receipt.
- We are aware of the circumstances when we can extend the time limit to respond to a request.
- We understand that there is a particular emphasis on using clear and plain language if we are disclosing information to a child.
- We understand what we need to consider if a request includes information about others.

Topic #4:
Breach Compliance

Art. 33 GDPR - Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.
2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.
3. The notification referred to in paragraph 1 shall at least:
   (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
   (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
   (c) describe the likely consequences of the personal data breach;
   (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.
5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

Art. 34 GDPR - Communication of a personal data breach to the data subject

1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.
2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).
3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:
   (a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
   (b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;
   (c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.
4. If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.

Data Breach Requirements

- What is a breach? A "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data".* (*Art 4(12) GDPR*)
- Must be notified to the relevant supervisory authority without undue delay and, where feasible, within 72 hours, **unless** the breach is unlikely to result in a high risk to the rights and freedoms of individuals (*Art 33(1) GDPR*)
- All breaches must be documented, whether or not notified (*Art 33(5) GDPR*)
- When the breach is likely to result in a high risk to the rights and freedoms of individuals, the breach must be notified to the data subject without undue delay, subject to limited exceptions (*Art 34(1) GDPR*)
- There is guidance from the European Data Protection Board and ICO on personal data breach notification

Session #2: Compliance with California Consumer Privacy Act

Overview

- Scope
  - Whom does the CCPA regulate?
  - Whose data is protected?
  - What data is protected?
- Timing
  - When will the CCPA be enforced?
  - When will implementing regulations be issued?
  - Might the statute be amended before the enforcement date?
- Substance
  - Data subject rights
  - Basic Requirements
- Enforcement
- Compliance Preparation

Scope: Who is Regulated?

- **Regulated entities: businesses operating in CA (or entities they control or are controlled by) that:**
  - have annual gross revenues in excess of $25 million;
  - annually buy, sell, receive or share for commercial purposes personal information of 50,000 or more CA consumers or devices; or
  - derive 50% or more of annual revenues from selling CA consumers' personal information
- **Exempted entities: businesses that have *neither:***
  - Nonprofit companies
  - Businesses that have no physical presence or affiliates in CA *and* no commercial activity in CA

Scope: Whose Data is Protected?

- Consumers, which are defined as:
  - Any “natural person who is a California resident”
    - *E.g.*, individual customers, employees, website visitors
  - Includes individuals domiciled in CA who are outside the state for a temporary or transitory purpose
- Excludes:
  - An individual who is in CA solely for a temporary or transitory purpose

Scope: What Data is Protected?

- **"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"
  - inferences drawn from any such identifiable information … to create a profile about a consumer
- **Examples (*not* exclusive):**
  - Identifiers: names, addresses, email addresses, Social Security numbers, driver's license numbers, IP addresses
  - Geolocation data
  - Biometric information
  - Characteristics of protected classes (race, religion, etc.)
  - Records of purchasing history or tendencies
  - Internet or other electronic network activity, such as browsing history

Exemptions for Personal Data Regulated Under Other Privacy Laws

- **Exempted Medical Information**
  - Medical information governed by the CA Confidentiality of Medical Information Act
  - Protected health information collected by a HIPAA covered entity or business associate
  - Information collected as part of a clinical trial if the trial is subject to: (i) the Federal Policy for the Protection of Human Subjects (Common Rule); (ii) the Food & Drug Administration's human subject protection requirements; or (iii) good clinical practice guidelines issued by the International Council for Harmonisation
- **Exempted Financial Information**
  - personal information regulated under the Gramm-Leach-Bliley Act's privacy provisions; the CA Financial Information Privacy Act, or used to generate a consumer report regulated under the Fair Credit Reporting Act
- **Personal Information Regulated Under the Driver's Privacy Protection Act**

NOTE: none of these exemptions applies with respect to liability for data security breaches

Timing: When Will the CCPA Be Enforced?

- Enforcement begins by July 1, 2020 (possibly sooner)
  - Implementing regulations from the CA Attorney General must be published by July 1, 2020
  - Enforcement begins on the earlier of:
    - Six months after the AG's regulations are published
    - July 1, 2020
- **Current activity:**
  - Legislation: several bills are pending to amend the existing CCPA
  - Regulatory proceedings: the AG is holding public hearings and soliciting comments on the statute's proper interpretation and implementation

Consumer Rights: Overview

- **Like the GDPR, the CCPA grants "consumers" substantial rights in relation to their personal information, including the right to:**
  - Obtain a list of the types of personal information a business has collected about them;
  - Review that information
  - Obtain a record of all sales or other disclosures of the information to third parties, including
    - Description of the receiving third parties
    - Statement of purpose of each sale or disclosure
  - Direct that the information not be sold or shared with third parties
  - In certain circumstances, direct that the information be deleted
  - Obtain goods or services without price or other discrimination due to the exercise of privacy rights
- **Unlike the GDPR, the CCPA does not require opt-ins, except to sell personal information concerning a child under age 16 (parent or guardian must opt in for child under 13)**

Special Right: Opting Out of Sales of Personal Information

- **What is a "sale" of personal information under the CCPA?**
  - Any disclosure (including provision of access) or communication of information, in any form
  - In exchange for "monetary or other valuable consideration"
- **A businesses that sells personal information must:**
  - State in a public-facing privacy notice what categories of personal information are sold
  - Post a "Do Not Sell My Personal Information" opt-out button on its website home page
  - Not seek consent to sell from a consumer who has opted out for 1 year after that opt-out
  - Upon a consumer's request, provide a report describing:
    - The specific types of that consumer's information sold
    - The categories of persons to whom it was sold
    - The business purpose for the sale(s)

Non-Sale Disclosures of Personal Information

- **Disclosures to Service Providers** need not be specifically reported to consumers
- **Disclosures to other nonaffiliates ("Third Parties")** must be tracked so that reports may be provided to consumers
- **"Service provider"**: a for-profit entity that processes personal information for a business pursuant to a written contract," provided that the contract limits the retention, use, and disclosure of the information
- **"Third party"**: an entity that is not a Service Provider
- **Legal Responsibilities**:
  - Service Providers are contractually bound to protect personal information they receive from a business
  - Third Parties may not sell a consumer's personal information they purchased unless the consumer is given an explicit opportunity to opt out of the sale and declines to do so

Required Online Privacy Notices

- **Every business regulated under the CCPA must post on its website a notice, which may be included in an online privacy policy, describing:**
  - A consumer's privacy rights under the CCPA (e.g., to access, prevent the sale of, and be informed of disclosures of the consumer's personal information)
  - The categories of personal information collected from consumers in the past 12 months
  - The types of personal information the business has sold in the past 12 months (or the fact that the business has not sold any personal information in that period)
  - The types of personal information the business has disclosed for a business purpose in the past 12 months (or the fact that the business has not made such disclosures in that period)
- **The notice must be updated every 12 months**

Required Responses to Consumer Requests

- **Businesses must provide at least two means for consumers to make requests for reports on what personal information about them has been collected and/or disclosed/sold, including:**
  - A toll-free number
  - A website address (assuming the business has a website)
- **When requests are received, a business must:**
  - Determine if the request is a "verifiable consumer request" (*i.e.*, made by the individual to whom the personal information at issue pertains)
  - Provide the consumer, free of charge, with the requested report within 45 days of receiving the verifiable consumer request
    - The report must cover the 12 months preceding the date the request is received
    - An additional 45 days may be used to respond if the consumer is informed within the initial 45 days that the response period is being extended

Enforcement: Attorney General Actions

- **Consumers may sue for damages from a data security breach of personal information as defined under the CA data security statute**
  - Consumers must provide alleged offender with notice and a 30-day opportunity to cure prior to filing suit
  - Consumers may recover the greater of (i) statutory damages ranging from $100 to $750 per consumer per incident or (ii) actual damages
- **The CA Attorney General will enforce the CCPA's substantive requirements**
  - The AG may initiate actions against businesses for:
    - improperly selling, storing or sharing personal information
    - failing to provide required notices/reports to consumers
    - otherwise violating the prescriptions or prohibitions of the CCPA
  - Companies found liable in an AG action may be fined a civil penalty of not more than $2,500 for each violation, or $7,500 for each intentional violation

CCPA Compliance: Where to Start?

Map Your Data

- **Identify what personal information about CA residents you collect**
- **Locate all CA resident personal information you maintain**
- **Examine and categorize all uses of the information**
  - For what purposes is the information used?
  - How necessary are those uses?
  - Who are the users of the information?
- **Evaluate the security protections applied to the information**
- **List all disclosures made or planned**
  - Who has access to the information?
  - Who receives it and how? Under contract or otherwise?
  - Are any disclosures made for valuable consideration and thus are “sales”?

Prepare a New Public-Facing Privacy Notice

- **Review any current public-facing privacy notice/policies**
- **Identify gaps to fill to cover all CCPA-required disclosures**
- **Be specific about consumer rights of access, reporting, deletion, etc.**
- **Include toll-free number and website address for consumers to raise questions and submit requests**

Offer Opt-out from Sales of Personal Information

If you sell or contemplate selling any CA residents' personal information:

- Provide a clear and conspicuous link on your Internet home page titled: "Do Not Sell My Personal Information"
- Enable a consumer to easily opt out of your sale of the consumer's personal information by clicking through that link
- Record and honor each opt out
- Refrain for 1 year following a consumer's opt out from seeking consent to sell the consumer's personal information

Establish Internal Policies and Procedures

- **Create internal policies so your workforce knows how to properly:**
  - Identify and track CA residents' personal information
  - Respond to consumers' questions about their personal information and its privacy and security
  - Authenticate CA residents to determine that their requests are verifiable consumer requests
  - Fulfill requirements in response to consumer requests for access, reports of data collection and sharing, data deletion, etc.
  - Retain information needed to respond to consumer requests for reports on what personal information was collected, to whom it was sold or otherwise disclosed, and the purposes for each sale or disclosure
- **Assess and upgrade the security measures applied to personal information**
- **Review and enhance your data security breach response plans**

Train Your Workforce

- The CCPA mandates that businesses "ensure that all individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance" with the CCPA are *informed of all the CCPA requirements.*
- Training is THE key to compliance
- Design an effective training program:
  - Make it interactive
  - Make it relevant (every person has personal information!)
  - Pose questions to be answered by participants
  - Test participants' retention of the information
- Conduct refresher trainings at least annually, and whenever legal changes or policy updates are made

Document and Review Relevant Activity

- Keep records of interactions with CA residents, including (but not limited to):
  - Inquiries posed – were they effectively answered?
  - Requests made – were they verifiable consumer requests?
  - Responses provided – were verifiable requests fulfilled in timely and adequate manner?
  - Complaints made – how were these addressed, were they escalated to management?
- Reevaluate compliance on a regular basis
- Make improvements based on:
  - Mistakes made
  - Flaws or gaps detected
  - Knowledge acquired
  - Technology improvements

Questions & Discussion

Speakers

Michael Kallens, Associate General Counsel, Washington, DC

Michael.Kallens@nasdaq.com, +1 301.978.8423

Mr. Kallens is a Senior Associate General Counsel in Nasdaq's Office of General Counsel and a senior member of Nasdaq's Global Ethics and Compliance Team. He has led industry working groups on developing best practices for corporate ethics programs and is a frequent speaker on ethics and compliance topics. In 2014, Mr. Kallens received the Outstanding In-House Counsel Award from the Association of Corporate Counsel-National Capital Region for his work in the area of corporate ethics and compliance.

Rob Bratby, Partner, London

rob.bratby@arnoldporter.com, +44 77 3831 2629

Mr. Bratby provides regulatory and transactional counsel in the telecoms, media and technology sectors and on data privacy and cyber security issues more widely. He has advised European, US and global companies on data privacy and GDPR compliance and has counselled companies on their responses to data breaches. Currently resident in London, he lived and worked in Singapore 2011-2016. He is ranked by Chambers, Legal 500 and Who's Who Legal as a leading data protection lawyer. He curates the firm's 'Digital Watcher' blog and speaks and writes widely on international regulatory issues. His experience before joining the firm includes law firm leadership positions in both Europe and Asia, working in-house at a telecoms operator and working for the UK telecoms regulator.

Nancy Perkins, Counsel, Washington, DC

nancy.perkins@arnoldporter.com, +1 202.942.5065

Ms. Perkins focuses her practice on litigation, regulatory compliance, and consulting on emerging policy issues, with a principal focus on data privacy and security. She regularly advises clients on compliance with a wide range of data protection requirements at the federal and state levels, including rules applicable to online communications and transactions as well as all types of uses and disclosures of medical, financial, and other sensitive personal information. She has deep background in international law and advises clients on the cross-border transfers of personal data, including under the GDPR and CCPA, as well as broader issues arising under the rapidly developing framework for global legal protection of personal information.