GDPR and the Rise of Heightened Privacy Regulations

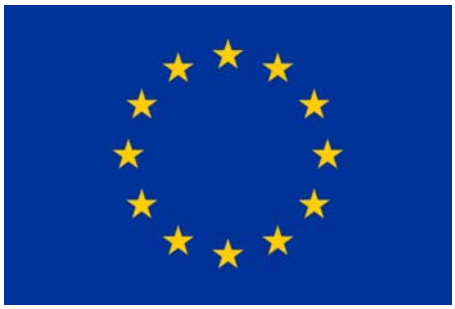
Presented by

Webb McArthur
Hudson Cook, LLP

NAFCU

HUDSON COOK

What is this "GDPR"?



- The **General Data Protection Regulation** ("GDPR") 2016/679 of the European Union ("EU").
- Provides data protection and privacy protections to individuals in the EU: fundamental rights in the EU.
- Repealed the 1995 Data Protection Directive (95/46/EC).
- Came into force on May 25, 2018, after 2 year transition period.
- Penalties of up to greater of 4% of revenue or €20M (USD$23M+).

NAFCU

HUDSON COOK

Overview of EU law

- GDPR is a "**regulation**."
- Passed by the European Parliament.
- Working Party 29 and European Data Protection Board.
- European Data Protection Supervisor.
- Member State (28, soon to be 27) Parliaments.
- Member State Data Protection Authorities.

NAFCU

HUDSON COOK

What does the GDPR regulate?

- Regulates the "processing" of "personal data."
  - **Processing** includes any operation performed on personal data.
  - **Personal data** is any information relating to an identified or identifiable data subject (person).
  - What about data that is encrypted, anonymized, or "pseudonymized"?
- Processing can be by a "controller" or a "processor."
  - A **controller** determines the purposes and means of processing.
  - A **processor** processes on behalf of a controller.

NAFCU

HUDSON COOK

Common Misconceptions about Scope

For a US business, GDPR is **not** triggered simply by:

- Operating a website that is accessible in the EU.
- Conducting business with EU citizens that are located in US.
- Collecting email addresses from visitors to your website.

Also, a change from the old Directive: processors are directly regulated by GDPR (not just "processor follows controller"), and each should independently conduct applicability analysis.

NAFCU

HUDSON COOK

Territorial Scope

1. Where the processing is "in the context of" activities of an entity **established in the EU**, even if processing is not in the EU.
    - Does not require data subject in the EU.
    - Question is *not* just whether you are established in the EU or whether you process data in the EU.
        - Establishment implies "effective and real exercise of activity through stable arrangements." Legal form is not dispositive.
        - "In the context of": Inextricably linked? Related to?

NAFCU

HUDSON COOK

Territorial Scope

2. Where the entity is not established in the EU but **offers goods or services to individuals in the EU**.
    - "*Envisage*" offering good or services and not "mere accessibility" of a website.
    - Relevant factors may include: use of non-home country EU language, EU currency, targeted advertising, EU or EU MS website domain, or paid inclusion of a site on a local search engine.
    - Any individual physically in the EU.
    - No payment requirement.

NAFCU

HUDSON COOK

Territorial Scope

3. Where the entity **monitors the behavior** (in the EU) of individuals in the EU.
    - Again, anyone present in the EU but only with regard to behavior in the EU.
    - Monitoring of EU behavior includes tracking of online activities for subsequent profiling of personal preferences, behaviors, or attitudes.
4. Where the law of an EU Member State applies by virtue of **international law**.

NAFCU

HUDSON COOK

Lawfulness of Processing

- Data subject has given consent.
- Necessary for the performance of a contract with the data subject or to take steps for a data subject before entering into a contract.
- Necessary for compliance with a legal obligation to which the controller is subject.
- Necessary to protect the vital interests of a natural person.
- Necessary for the purposes of legitimate interests pursued by the controller or a third party except where such interest are overridden by interests or data protection rights of the data subject.

NAFCU

HUDSON COOK

Consent to Collect

- "Consent" means "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or clear affirmative action, signifies agreement to the processing of personal data."
- Must be clearly distinguishable from other consents, intelligible, in an easily accessible form, and in clear and plain language.
- Implied consent (e.g., cookies) may not work.
- Must be as easy to withdraw as to provide.

NAFCU

HUDSON COOK

Right to Information

- General “privacy notice” disclosure requirement upon collecting data (within one month or before communicating with data subject or another party).
- List of information for disclosure includes information about the controller, purposes of processing the data, categories of data, lawful basis for processing, and intended retention of data.

NAFCU

HUDSON COOK

Right to Access

- Right to be informed whether data being processed.
- If so, must also provide purposes, categories of data, recipients or categories, envisaged period of storage, recitation of other rights, source information, and whether automated profiling utilized.
- Can get one free electronic copy of all data.

NAFCU

HUDSON COOK

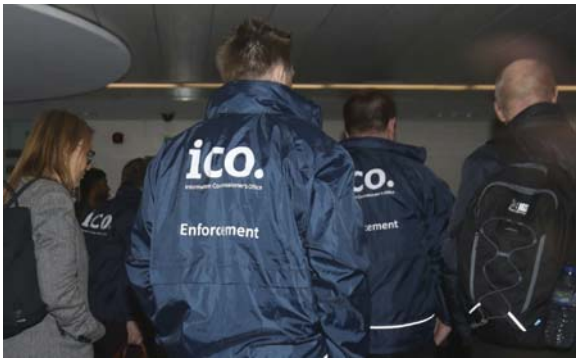
Right to Object

- If processing *based on legitimate interests of the controller*, data subject can object and, unless the controller demonstrates compelling legitimate grounds overriding the data subject's interest, must cease processing.
- Data subjects can also object and be removed from *direct marketing purposes*.

NAFCU

HUDSON COOK

Right to Erasure



- Or "right to be forgotten."
- Must erase if requested where:
  - Personal data no longer necessary.
  - Processing based on *consent* now withdrawn.
  - Data subject objects and there is *no overriding legitimate grounds* to process.
- Must cease dissemination.

NAFCU

HUDSON COOK

Right to Data Portability

- Right to obtain and reuse data (including for own purposes) by transferring data across IT environments.
- Applies where processing is by *consent* and processing is automated.
- Where feasible, can request direct transfer to another controller.

NAFCU

HUDSON COOK

Other Issues Related to Consumer Rights

- Profiling:
  - Specific situations require consent rather than other permissible reasons to process.
  - Also have right not to be subject to automated profiling decision except where contractually or legally required.
- Special data categories have processing restrictions (e.g. age can provide consent).
- Current rights in the Directive to correct, delete, and block data remain.

NAFCU

HUDSON COOK

Other Obligations

- Appoint a Data Protection Officer if core activities consist of processing activities which require regular and systematic monitoring of data subjects on a large scale.
- Notification to DPA of Data Breach ("breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed")
- Data Security Program
- Confidentiality

NAFCU

HUDSON COOK

How else might the GDPR affect you?

1. If **data is transferred** to you from a processor or even a controller subject to GDPR.

- GDPR limits cross border data transfers – may only transfer data if:
  - Adequate level of protection (Privacy Shield – will have to watch)
  - Binding Corporate Rules
  - Standard Corporate Clauses
- Derogations for occasional and non-repetitive transfers with a lawful basis for the processing.

NAFCU

HUDSON COOK

How else might the GDPR affect you?

2. If you **engage a processor** that is subject to GDPR.

- Art. 28 requires:
  - *Controllers* may engage only processors that can ensure its full compliance.
  - *Processors* may process only by written contract specifying details of processing relationship, ensuring compliance with security and data breach requirements, and will assist the controller in its compliance.
- Processor might decide to comply with GDPR for all engagements.
- GDPR does not require processors to obligate their customers to comply with GDPR, so may become matter of contract.

NAFCU

HUDSON COOK

Other Global Developments

- China: Personal Information Security Standard (eff. 5/1/18)
  - In development: technical cyber and national security standards.
  - "Sensitive personal information" broader than GDPR: any data that can cause harm to a person, property, reputation, or health.
  - Consent required for more circumstances than GDPR.
- Brazil: LGPB (eff. 2/14/20)
  - Very similar to GDPR.
  - More bases for lawful processing than GDPR (including protection of health and credit).
- Barbados: draft Data Protection Act

NAFCU

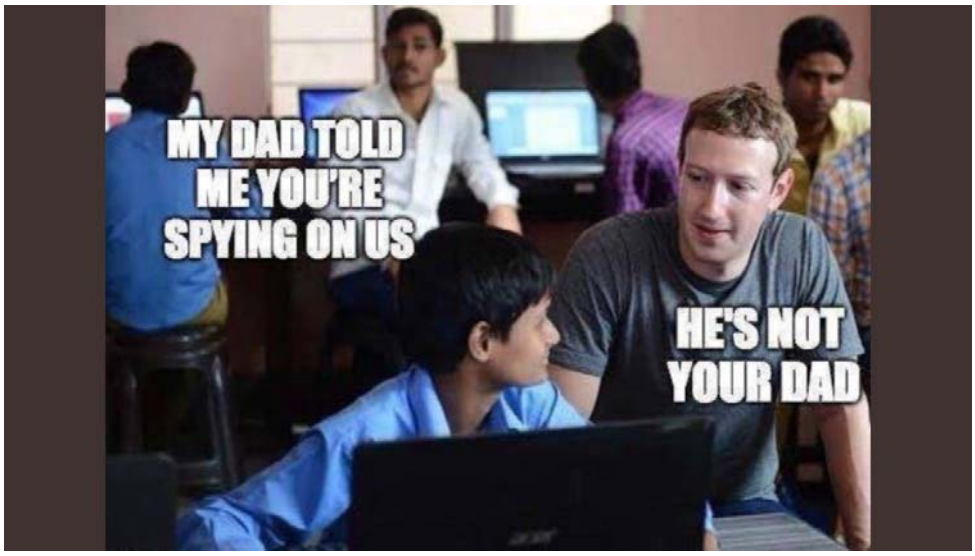
HUDSON COOK

US Developments

- California Consumer Privacy Act (eff. 1/1/2)
  - "Personal information" broader than GDPR in some ways,
  - Specific to CA residents, but broad "business" triggers (no "for profit" requirement).
  - Consumer rights (1) to information (when data collected and transferred), (2) to opt out, and (3) to delete.
  - Private right of action for data breach provisions.
  - Rulemaking and enforcement by AG; expecting further amendments.
- Vermont Data Broker Law
- Chicago: Personal Data Collection and Protection Ordinance

NAFCU

HUDSON COOK



NAFCU

Where are we going?

- A culture shift: moving toward generally applicable, comprehensive data regulation.
- Monitor developments!
- While it may not be advised to comply with laws like GDPR if they don't apply to you, you should start thinking about:
  - Consider transparency and fairness, particular consent
  - Privacy by design and by default
  - Data minimization
  - Data inventory and mapping (fielding data)
  - Marketing: What exactly are you doing? With what data? What might consumers think about your marketing?

NAFCU

HUDSON COOK

Resources

- GDPR full text: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN
- EC info page: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en
- Article 29 working party: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358
- EDPB: https://edpb.europa.eu/news/news_en
- UK ICO info page: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/whats-new/

NAFCU

HUDSON COOK

Questions?

NAFCU

HUDSON COOK

Contact Information

Webb McArthur
Hudson Cook, LLP
1909 K Street, N.W.
4th Floor
Washington, DC 2006
(202) 715-2012
wmcarthur@hudco.com

NAFCU

HUDSON COOK