Arnold & Porter

# Basics of EU General Data Protection Regulation (GDPR) for U.S. Government Contractors

**Craig Schwartz**

**NDIA Procurement Division Meeting (Oct. 16, 2018)**

# GDPR & EU Law Background

- GDPR is an EU regulation governing the (i) processing of (ii) personally identifiable data belonging to (iii) a natural person
  - Entered into force on May 25, 2018
  - Intent is to strengthen and unify data protection rules across the EU
- GDPR supplanted EU Data Protection Directive No. 95/46/EC, which had been in place since 1995
  - EU regulations have binding legal force in every member state. They enter into force in all member states on a set date (here, May 25, 2018).
  - By comparison, EU directives specify results each member state must achieve. The member states have discretion to decide how to achieve those results through national laws.

# GDPR & EU Law Background

- GDPR proclaims "the protection of personal data" to be a "fundamental right and freedom," Art. 1 ¶ 2
- Establishes individual rights for "data subjects," Arts. 12-23
  - Touchstone is transparency as to how a subject's data is being processed
  - Includes the "right to be forgotten," Art. 17
- Imposes new data breach self-reporting requirements
  - Notify supervisory authority "without undue delay and, where feasible, not later than 72 hours after having become aware," Art. 33
  - Notify data subject of "high risk" breaches "without undue delay" in "clear and plain language," Art. 34
- Creates a **private right of action** to recover damages arising from non-compliance, Art. 82 ¶ 1
  - Individuals may delegate this right to a (i) "not-for-profit" (ii) "public interest" organization (iii) "active in the . . . protection of data subjects' rights and freedoms"

# Definitions

- “Processing” includes the storage of data, including by third parties (in which event, there is a “controller” and a “processor”).
- GDPR imposes different obligations on the controller and processor of personally identifiable data.  An organization can be both.
- GDPR does not apply to wholly anonymized data, as it is not “personally identifiable.”
- GDPR largely does not apply to “pseudo anonymized” data (in which the data may be attributable to an individual using additional information) unless specified information safeguarding and segregation requirements are not satisfied.
- “Natural persons” does not include legal entities (*i.e.*, corporations).

# GDPR's Reach

- GDPR applies to the data of persons in the 28 EU member states
  - Extends to the three non-EU EEA states of Iceland, Liechtenstein, and Norway
- The European Commission has recognized the following jurisdictions as maintaining "adequate" privacy protections for data transfers out of the EU (non-exhaustive list):
  - Argentina, Canada, Israel, New Zealand, Switzerland, and Uruguay

# GDPR's Reach

- Australia and the U.S. **are not recognized**, although data transfers to the U.S. may be conducted if:
  - The organization creates and enforces "binding corporate rules" governing intra-company transfers between the EU and U.S. affiliates, approved by an EU member state's designated regulator (UK is generally the fastest);
  - The EU sender and U.S. recipient enter into a data transfer agreement with "model clauses" preapproved by the European Commission (most popular approach); or
    - Best practice is to have a separate DTA for each EU subsidiary with the U.S. parent
  - The transfer is compliant with the July 12, 2016 "Privacy Shield" framework adopted by the EU and U.S. governments
    - The framework, administered in the U.S. by the Commerce Department and enforced by the Federal Trade Commission (FTC), provides for more limited transfer rights than full European Commission recognition
  - In some circumstances, companies may outsource management of international data transfers to third-party cloud providers

# GDPR's Reach

- A U.S. employee remotely accessing data maintained in the EU is considered a data transfer to the U.S.
- Both the model clauses and Privacy Shield are currently under legal challenge in the EU as insufficient protection for international data transfers
- California recently passed the Consumer Privacy Act of 2018, A.B. 375
  - Set to go into effect in 2020
  - Has been described by some commentators as "GDPR-lite"
  - The European Commission is unlikely to recognize full transfer rights to California but not other U.S. states since, as a practical matter, the data could be re-transferred to other U.S. states once in California

# GDPR's Reach

- As applied to a U.S. company, the jurisdictional hook (from the Data Protection Directive to GDPR) has shifted
  - Pre-GDPR Test: Office or equipment in EU (including an app)?
- GDPR applies to "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]," Art. 3 ¶ 1
  - In plain English, GDPR applies if:
    - Physical presence in EU beyond mere website (*e.g.*, design or manufacturing operations), *see* Recital 22 (defining "establishment");
    - Actively market goods or services in EU; or
    - Track/profile persons in EU
- At bottom, is the company making money from processing the personal data of persons in the EU?

# GDPR's Reach

- Possible Indicia of GDPR Jurisdiction:
  - Display different languages on website depending on where the user loads the page?
  - Accept Euros or other EU member state currencies for payment?
  - Use cookies to track/profile visitors to website from EU member states?
  - Send marketing emails into EU?
  - Mere EU accessibility of website is **not** a sufficient basis for jurisdiction
- EU Privacy and Electronic Communications (PEC) Directive No. 2002/58/EC separately regulates privacy rights relating to electronic communications
  - Covers marketing calls, emails, faxes, and texts
  - PEC Directive likely to be supplanted by updated EU regulation in near future
- For U.S. government contractors, be cautious as to electronic contacts with U.S. service members stationed in Europe or with NATO allies

# Implications of Brexit?

- The UK is expected to adopt a Swiss or Canadian approach following Brexit, but the European Commission would need to recognize the approach as adequate
  - Alternatively, the UK likely would seek a separate framework for data transfers akin to the EU-U.S. Privacy Shield

# Why Does GDPR Matter?

- Prescribes fines of **up to € 20 million or 4% of global annual turnover** (whichever is higher) for more serious violations, and fines of up to € 10 million or 2% of global annual turnover (whichever is higher) for less serious violations
  - Magnitude of fines is discretionary
  - Enforcement is expected to be harsher in civil law jurisdictions than in common law jurisdictions
  - On the day GDPR went into effect, an Austrian privacy watchdog filed complaints seeking approximately $9.3 billion (U.S.) in fines from Alphabet (*i.e.*, Google) and Facebook (including Instagram and WhatsApp)

# GDPR Core Requirements

- An organization must have a "lawful basis" to process personal data. Art. 6 ¶ 1 of the regulation specifies six bases:
  - (a) "the data subject has given consent to the processing of his or her personal data for one or more specific purposes"
  - (b) "processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract"
  - (c) "processing is necessary for compliance with a legal obligation to which the controller is subject“
    - *See also* Art. 49 ¶ 1(e)
    - It is not yet clear whether compliance with a U.S. legal obligation is sufficient
    - There may be variation in the interpretation of this and other GDPR provisions by UK/Irish courts vis-à-vis German/French courts
  - (d) "processing is necessary in order to protect the vital interests of the data subject or of another natural person”

# GDPR Core Requirements

- (e) "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller"
- (f) "processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child“

- Caution:  Be wary of relying only on consent
  - Consent has specificity requirements, cannot be bundled in unrelated documents, and **can always be withdrawn**
  - If applicable, parrot bases such as “necessary for the performance of a contract to which you are a party” or “compliance with a legal obligation” in a privacy notice to data subjects
- When processing personal data, the organization must meet what effectively is a “reasonable care” standard as to data security, Art. 32

# Additional Risk Areas

- Art. 9 identifies “Special Categories of Personal Data” that may not be processed unless a specified exception applies
  - Consent is a specified exception
  - Here especially, reliance on withdrawable consent presents risk
- The special categories are:
  - "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership"
  - "genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health[,] or data concerning a natural person’s sex life or sexual orientation“
- GDPR imposes a requirement on “controllers” to maintain a compliance audit trail, Art. 24 ¶ 1
- GDPR is a floor, not a ceiling
  - *E.g.*, member states may establish additional “special category” protections

# Best Practices for U.S. Companies Generally

- Evaluate whether, and to what extent, GDPR applies
- If GDPR applies, decide whether to extend the protections globally or only to covered EU activities
  - Caution that the U.S. FTC polices violations of the EU-U.S. Privacy Shield and representations by U.S. companies regarding the extent of their privacy practices
  - There is risk to enshrining GDPR protections in a privacy policy (*e.g.*, the right to be forgotten), where operationalizing the protections requires expensive changes to enterprise systems/databases
    - Don't promise what you can't deliver. **Legal and IT must coordinate!**
  - There must be a business case to extending rights to customers that are not required (*e.g.*, marketing value or a benefit of uniform policies)
    - Do you want to limit data processing to those that opt-in?
    - On demand, can you provide subjects their data? Correct data errors? Implement the right to be forgotten?

# Best Practices for U.S. Companies Generally

- If GDPR applies, or if business warrants extending its protections:
  - Update privacy policy for employees within organization (posted on corporate intranet and/or in employee handbook), and for data subjects external to organization
    - Post or send privacy notice to external data subjects with ability to correct data or opt-out of data storage
    - Require affirmative opt-in to new policy with no pre-checked box
    - Going forward, default to opt-out for storage of new personal data (unless there is another basis for storing the data besides consent)
  - Comply with EU-U.S. Privacy Shield (data privacy) and, if a government contractor, NIST SP 800-171 (cybersecurity)
  - Assign someone the responsibility of “Data Protection Officer” (or its functional equivalent)
    - May contract for this function outside of the organization if certain conditions are met

# Best Practices for U.S. Government Contractors

- Where GDPR jurisdictional indicia are met:
  - Prime contractors should contractually flow GDPR obligations down to suppliers/service subcontractors who "process" personally identifiable data "controlled" by the prime contractor, whether through:
    - Certifications (as described in Art. 42); or
    - Codes of Conduct (as described in Art. 40)
  - Likewise, prime contractors should request certifications of GDPR "processor" compliance from preexisting suppliers/service subcontractors
  - Art. 28 specifies the obligations on a data processor
- U.S. contractors should beware of inadvertent exposure to GDPR processor obligations when acting as a supplier/subcontractor to an EU "controller" (including an EU affiliate)

# Best Practices for U.S. Government Contractors

- Action Items:
  - Determine whether EU consents obtained for compliance with U.S. reporting requirements that were sufficient under the prior Data Protection Directive are still sufficient under GDPR
    - Issues relating to EU member state, particularly German, blocking statutes remain
    - These issues arise especially in the context of U.S. FCPA enforcement
  - **Ensure privacy notices state upfront**: "We will share information as needed to comply with regulatory reporting requirements in any country in which we operate."
  - Execute a separate data transfer agreement with preapproved "model clauses" for each EU subsidiary with the U.S. parent
  - When a prime contractor, restrict subcontractor access to unneeded personally identifiable data in your control
  - When a subcontractor, restrict exposure to unneeded personally identifiable data in the prime contractor's control

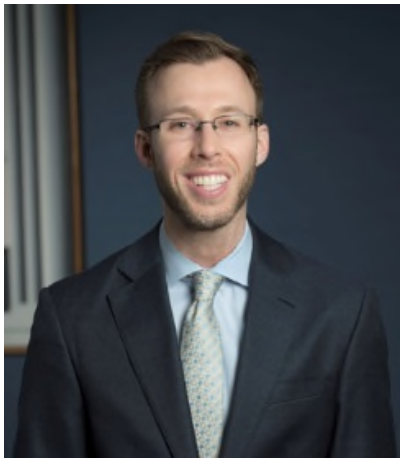
# Best Practices for U.S. Government Contractors

- Interplay of GDPR and DFARS Clause 252.204-7012, “Safeguarding Covered Defense Information and Cyber Incident Reporting”
  - U.S. reporting protocols for Defense Industrial Base data covered by international privacy protections are still developing
  - This is an area to watch for Defense Procurement Acquisition Policy (DPAP) guidance going forward
- More generally, beware of risks relating to international supply chains in light of U.S. regulatory reporting requirements *(e.g.*, human trafficking reporting)
  - EU courts, especially French and German courts, may not agree to personally identifiable data transfers to satisfy U.S. reporting requirements
  - If no exception or lawful basis for transfer applies, transfer requests may be made under the Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters
  - Turnaround times under the Hague Convention may be too slow for U.S. regulators’ tastes

# Closing Thoughts

- Yes.  GDPR can reach U.S. companies, including government contractors.
- No.  The sky is not falling.  GDPR does not stop you from doing almost anything, so long as you are transparent.
- While GDPR fines can be massive, they are **discretionary**
  - It is too early in GDPR enforcement to forecast fine magnitude
  - Depending on their degree of EU exposure, some contractors should consider undertaking a voluntary “privacy impact assessment”
  - For others, it may be prudent to have a risk mitigation plan in place (even if not fully developed) that meets the “spirit” of GDPR
  - This may allow a contractor to request leniency because it took good faith steps to mitigate GDPR non-compliance risk
  - UK and Irish courts may be more likely than German and French courts to credit partial GDPR compliance in assessing fines
- Keep relevant corporate leadership (GC, Risk Officer, and Board Audit Committee) apprised of how you are managing data privacy risk

# Contact Information



**Craig Schwartz**

**Arnold & Porter**

+1 202.942.6686

craig.schwartz@arnoldporter.com