# Law Firm GC Roundtable

## Dad Are We There Yet? The Journey to GDPR Compliance – But How Did We End Up in California?

Steven M. Puiszis
Hinshaw & Culbertson LLP

**Chicago, IL**

**July 26, 2018**

HINSHAW

# NY Times: Europe's Data Protection Law Is a Big, Confusing Mess

- The law is staggeringly complex.
- The regulation is intentionally ambiguous, representing a series of compromises.
- What are often framed as legal and technical questions are also questions of values.
- No one understands the GDPR.

Source: https://www.nytimes.com/2018/05/15/opinion/gdpr-europe-data-protection.html

# GDPR – A Big Confusing Mess

- 99 Articles, 173 recitals with over 57,500 words
- Employs terms unfamiliar to many lawyers and business people
- 43 times longer than the Declaration of Independence
- 214 times longer than the Gettysburg Address
- Permits Member States to enact implementing legislation that modify, enhance or limit a number of its requirements

# Who's Ready for the GDPR?

- According to a survey published by Reuters on May 8th, seventeen out of twenty-four Supervisory Authorities "…said they did not yet have the necessary funding, or would initially lack the powers, to fulfill their GDPR duties."
- "Most respondents said they would react to complaints and investigate them on merit. A minority said they would proactively investigate whether companies were complying and sanction the most glaring violations.

Source: https://www.reuters.com/article/us-europe-privacy-analysis/european-regulators-were-not-ready-for-new-privacy-law-idUSKBN1I915X

# GDPR Readiness

Gartner has predicted that by the end of 2018 at least 50% of companies affected by GDPR will fail to fully comply.

Elizabeth Denham, UK Information Commissioner at the ICO:

- *“The first thing we are going to look at is, have they taken steps, have they taken action to undertake the new compliance regime”…*
- *"Do they have a commitment to the regime?*
- *"We're not going to be looking at perfection, we're going to be looking for commitment.“*

Source: http://www.bbc.com/news/technology-43657546

# Compliance/Risk Management Questions

- Does the GDPR apply to your firm?
- What GDPR data do we have? Does any of it qualify as sensitive personal data?
- Matter data, Marketing data, Human Resources data, Security data.
- Where is GDPR data located and stored; who can access the data (lawyers, staff and third party vendors); do they all need access; how is access obtained?
- What risks exist at each access point.
- How do you receive GDPR data; what do you or a third party do with that data; do you transfer any of it outside the EU?
- Do you need to retain all the GDPR data in your possession; do you have a data retention schedule applicable to GDPR data; are you following that retention schedule and are you securely disposing of electronic data? Can you automate tagging, and data destruction routines for GDPR data?

# Compliance/Risk Management Questions

- Do you need a GDPR Privacy Policy?
- Do you need to revise your website privacy policy and draft privacy notices for other uses such as engagements? Do you need a “cookie” popup? Do you need to draft privacy notices for your EU employees?
- Do you need to revise your engagement letter(s) to address any GDPR issue(s)?
- Do you need to revise your information governance policies/practices to comply with GDPR?
- Do you need to review and revise your agreements with third party vendors that have access to GDPR data?
- Do your systems have the capability to permit timely access, correction, restrict access, and/or erase all copies of GDPR personal information if necessary?

# Compliance/Risk Management Issues

- Do you need to review your breach response process/ plan to address GDPR breach reporting requirements?
- Do you need a specific EU records retention and data destruction policies?
- Does your record keeping meet the GDPR's requirements and can you demonstrate compliance with the regulation?
- Do you have a lawful basis is for processing GDPR data or for transfers of data outside the EU? What safeguards do you have in place for those transfers?
- Do you need a personal representative and/or data protection officer?
- Have you documented risk assessments in the past involving the use of new technologies or new procedures and the potential impact on client data? Will those meet the GDPR's requirement for data protection impact assessments?
- Have you considered and implemented privacy by design?

# GDPR – Background Information

- Data privacy is considered a fundamental human right in the EU.
- Replaces EU Data Protection Directive 95/46/EC.
- Intended to establish a uniform data privacy law across the EU.
- But permits Member States to impose additional conditions or safeguards, so there will be variations between countries.
- Applies to any sized entity – no small business exception.
- Authorizes potentially significant fines for serious violations—up to 4% of annual world-wide turnover or 20 million Euro whichever is greater.

# GDPR's Data Processing Principles

Personal data should be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specific, explicit and legitimate purposes and only processed in a manner that is consistent with those purposes
- Relevant and limited to what is necessary in relation to the purposes for which that information is processed (data minimization)
- Accurate, kept up to date, and that inaccurate information be deleted or corrected without undue delay
- Retained in a form that permits the identification of a person for no longer than is necessary for the purposes of its processing
- Processed in a manner that ensures the security of the personal information through appropriate technical and organizational measures

# GDPR's "Jurisdictional Hooks"

- Entities with an established presence in the EU (regardless of where the processing takes place).
- Entities that are not established in the EU if they either:

  1) Offer Goods or Services to Natural Persons in the EU (irrespective of whether payment is required).

  2) Monitor Behavior of Natural Persons taking place in the EU.

     a) Applies to natural persons, not citizens or residents.

     b) Mere website accessibility not enough.

     c) Household purposes (personal) exemption.

# GDPR Personal Data – Broader than Personally Identifiable Information

- *Any information relating to* an identified or identifiable natural person.
- An identifiable natural person is one who can be identified, *directly or indirectly,* in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, psychological, genetic, mental, economic, cultural or social identity of the natural person.
- Includes publicly available information.
- Does not apply to information about deceased persons.
- Excludes fully anonymized data.

# Special Categories of Personal Data

Greater protection granted to information that reveals a person's:

- Racial or ethnic origin.
- Political opinions, religious or philosophical beliefs, or union membership.
- Genetic or biometric data.
- Health, a person's sex life, or sexual orientation.

Does not include criminal convictions or offenses but processing of that information can only occur under the control of an official authority or pursuant to Union or Member State law.

# Processing of Data

- Any operation or set of operations performed on personal information or sets of personal data, *whether or not by automated means.*
- Includes collection, recording, organization, structuring, storage, adaptation, or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment, or combination, restriction, erasure or destruction of personal data.
- In other words, the GDPR applies to *anything* that an entity does to or with EU personal data, or that involves or affects that data.
- Includes manual processing of personal data in paper records that are part of a filing system (files structured in accordance with specific criteria).

# Data Processors and Controllers

- A processer is a natural or legal person, public authority or agency, or any other body that processes personal data on behalf of a controller.
- A controller is a natural or legal person, public authority, agency or other body that either alone or jointly with others, determines the purposes and means by which personal data will be processed.
- An entity can be both a controller and a processor concerning activities involving the same data.
- Given the independent professional judgment lawyers are required to exercise, law firms are data controllers.
- Controllers must maintain a record of its processing activities whereas processors only keep records of categories of processing activities.

# Lawful Basis for Processing Most Categories of Personal Data (Not Sensitive Personal Data)

A controller must have at least one lawful basis for any processing activity:

- Consent of data subject.
- To perform a contract or to take steps prior to entering into a contract at the data subject's request.
- The legitimate interests of the controller or a third party.
- To protect the vital interests of a data subject or another person.
- For the performance of a task in public interest or in the exercise of official authority vested in the controller.
- To comply with a legal obligation imposed by EU or a Member State law.

# Legitimate Interests

- Direct marketing (data subject has a right to object at any time).
- Preventing fraud.
- Internal administrative purposes.
- Insuring network and information security.
- Preventing unauthorized access to email systems or networks, and mitigating damage to electronic systems.
- Reporting possible criminal acts or threats to pubic security.
- Where a relevant and appropriate relationship exists between the data subject and the controller including where the data subject is a client or in the service of the controller (employee).

# Consent

- Must be freely given, specific, informed and unambiguous.
- Requires a clear indication of the person's decision either by a statement, or an affirmative action.
- Consent is not valid if a person is unable to refuse consent or unable to withdraw it at any time. Simple ways to withdraw consent must be provided.
- Consent is not valued if it is conditioned on the performance of a contract or provision of a service or benefit.
- Blanket consent to any and all processing activities is not specific.
- Opt-out consent inferred from silence or failure to respond not valid.

# Consent

- To be informed requires activities be explained in "clear and plain language" and presented in an intelligible and easily accessible form.
- Consent must be separated from other terms and conditions in a document or form and must be clearly distinguishable.
- Burden of proof on controller to show consent was validly obtained.
- Withdrawal of consent does not affect lawfulness of processing activities before the consent was withdrawn. Data subject must be advised on this point.
- Consent is not valid where there is a clear imbalance between the between a controller and a data subject. WP 29's guidance suggests this applies to an employer/employee relationship.

# Basis For Processing Special Categories of Data

- "Explicit" consent - except where prohibited by Union or Member State law.
- For the establishment, exercise or defense to legal claims.
- When the data has been "manifestly" made public by the data subject.
- To carry out obligations imposed by or to exercise rights under employment, social security, social protection law or a "collective" agreement.
- For purposes of preventative or occupational medicine, assessment of an employee's work capacity, medical diagnosis, provision or health or social care or treatments for the management of health or social care systems and services, or pursuant to contract with a health professional.
- To protect the vital interests of a person when the data subject is physically or legally incapable of providing consent.
- To meet a substantial public interest based on Union or Member State law.

# GDPR Data Security Requirements

- Controllers and processors are required to implement "appropriate technical and organizational measures to ensure a level of security appropriate to the risk."
- Risks to protect against – accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted stored or otherwise processed.
- Measures mentioned – encryption, pseudonymisation, ability to maintain ongoing confidentiality, integrity, availability and resilience of processing systems and services, ability to restore availability and access to data in a timely manner in the event of a “technical” incident; and regularly testing, assessing and evaluating the effectiveness of security measures.

# "Explicit" Consent

- The term is not defined or explained.
- Explicit consent required for:

    1) Processing special categories of sensitive data.

    2) Data transfers out of the EU.

    3) Fully automated decision making and profiling that produces legal effects on data subject.

- Article 29 Working Party Guidance: Refers to the way consent is expressed by data subject – data subject should "expressly confirm consent." (conceptually similar to documenting a conflict waiver)

# Data Subjects' Rights Under GDPR

- To be informed about the purposes for which their data is being processed, the lawful basis for processing, any third parties or categories of recipients with whom their data will be shared and the period of time it will be retained.
- To access their data (so long as it does not adversely affect the rights of others).
- To request inaccurate or incomplete information be corrected or completed (rectification).
- To delete their personal data (erasure); object to its processing or to restrict its processing.
- To transfer data to another controller (portability).

# Data Subject's Rights (cont'd)

- To be advised of the right to complain to a supervisory authority.
- To be informed of any automated decision making and/or profiling and the right to object to decisions based *solely* on automated decision making and/or profiling.
- Right to object to fully automated decision making – not applicable when processing is necessary for entering into or performing a contract, or when based on the data subject's explicit consent – but the data subject has a right to human intervention in these scenarios.
- To be advised about transfers of data outside the EU and the safeguards used in connection with any transfer.

# Right of Erasure

- Right triggered when:
  1) Data is no longer needed for the purpose it was originally collected or processed.
  2) Data subject withdraws his or her consent.
  3) When the data was unlawfully processed.
  4) To comply with a legal obligation imposed by EU or Member State law.
  5) When a data subject objects to processing and controller is unable to show compelling or legitimate grounds for processing which outweighs the data subject's rights.
- When data was made public by a controller, it is required to take reasonable steps to notify others processing the data about the request to erase the data including any links to, copies of, or replications of the data.

# Right of Erasure

- Data does not have to be deleted:

  1) When necessary for the establishment, exercise or defense of legal claims.

  2) To comply with a legal obligation imposed by Union or Member State law.

  3) To perform a task carried out in public interest or in the exercise of official authority.

  4) For public health purposes or for scientific or historical research.

  5) To exercise freedom of expressing and information.

# GDPR Rights Continued

- **Restrict Processing** – when accuracy is contested, or processing is unlawful and data subject opposes erasure and requests that it be restricted.
- **Notification** – Controller must communicate correction, restriction or erasure of data to each recipient of the data unless impossible or requires disproportionate effort.
- **Portability** – Only when processing was based on data subject's consent or necessary for performance of contract, and was performed by automated means. (Must not adversely affect another's rights).

# Privacy Notices - Content

- Controller's contact information and the contact information for any representative or data protection officer.
- Purpose and legal basis for processing.
- If legitimate interest(s) is/are relied upon, identify those interests.
- Recipients or categories of recipients of data.
- Details of cross border data transfers, existence/absence of an adequacy determination for the country where data is transferred, or safeguards used to protect.
- Applicable data retention period, or criteria used to determine length of time data is held.

# Privacy Notices – Content

- Data subjects' GDPR rights.
- Right to withdraw consent at any time.
- Right to lodge complaint with a supervisory authority.
- Whether processing is occurring pursuant to a statutory or contractual obligation, or if necessary to enter into a contract.
- Existence of automated decision making and "meaningful information" about the logic involved and consequences to data subject.
- Source of the personal data if source was a third party (not the data subject) and categories of data collected from any third party.

# Privacy Notices – Timing of Notice

- When collected from data subject – at the time of collection.
- When collected from third party – within a reasonable period of time, not later than one month after receipt unless used for communicating with data subject, then no later first communication. If it is to be disclosed to third party, then no later than first disclosure.
- Multiple notices not required – no need to send a privacy notice if data subject already has information.
- No need to send a notice if it is impossible or requires disproportionate effort or if it is subject to a statutory or professional secrecy requirement imposed by Union or Member State law.

# Privacy Notice - Format Requirements

- Written in clear and plan language in understandable terms.
- Provided in a concise, transparent, intelligent and easily accessible form.
- Can and should be provided in a variety of ways, *e.g.*, website, on applications or forms, engagement letters or attachments.
- If verbal, confirm in writing or email.

# GDPR – Vendor Management Requirements

- Controllers are only permitted to use processors that comply with the GDPR.
- Written agreements are required that mandate:

1) Processor is only permitted to process data in accordance with controller's documented instructions, including transfers outside the EU.
2) Imposes a confidentiality obligation on processor's employees with access to the data.
3) Requires the processor to implement and apply the GDPR's security measures for processing.
4) Requires the processor to assist controller in complying with data subjects' GDPR rights, meeting controller's breach notification and breach record keeping requirements, controller's obligations involving data protection impact assessments, obtaining approvals from a supervisory authority ("SA") and to cooperate with the SA.

# GDPR – Vendor Management Requirements

5) Requires the processor to return or destroy all data at end of relationship - at the controller's election.

6) To provide controller with information necessary to establish compliance with the GDPR (and allow access all records the controller is required to keep under the GDPR).

7) Allows and agrees to contribute to audits and inspections by the controller.

8) Prohibits the hiring or appointment of a subprocessor without prior consent of controller and that any subprocessor be subject to same terms as in processor's agreement with the controller.

9) Notify controller of personal data breach without undue delay.

10) Indemnification.

# GDPR Required Records - Controller

- Name and contact details of controller, any personal representative and/or DPO.
- The purposes for all processing activities.
- Description of the categories of data subjects and personal data processed.
- Categories of recipients with whom the data has or will be shared.
- Cross border data transfers and safeguards used for transfers.
- Data retention periods for categories of data.
- General description of technical and organizational security measures.

# GDPR Required Records - Processor

- Name and contact details of processor, any controller on behalf of which it is acting and any personal representative and/or DPO.
- Categories of processing carried out on behalf of a controller.
- Information about cross-border data transfers and safeguards used for transfers.
- General description of technical and organizational security measures.

# Small Business Record Keeping Exception – Controllers & Processors

- Employs less than 250 persons.
- Processing is not likely to result in a risk to rights and freedoms of data subjects
- Processing is occasional.
- Processing does not involve special categories of sensitive data or data relating to criminal convictions and offenses.

# Personal Representative

- Required for controllers and processors outside the EU unless:
    1) Processing is occasional.
    2) Processing activity does not involve *large scale* processing of sensitive data or data relating to criminal offenses.
    3) Processing is unlikely to result in a risk to rights and freedoms of natural persons taking into account its nature, content, scope and purposes.
- Serves as a point of contact for supervisory authorities and data subjects.
- When required, the PR should be appointed in a Member State where data subjects are located whose personal data is processed in relation to goods or services being offered.

# Data Protection Officer

- Controllers and processors are required to designate a DPO when its "core activities" involve either:
    1) Regular and systematic monitoring of data subjects on a "large scale"
    2) Processing special categories of sensitive data on a "large scale"
- Core activities are an entity's primary activities.
- DPO can be an employee or independent contractor.
- DPO should have expert knowledge of data protection.
- DPO to act independently and report to highest level of management.
- Large scale undefined.

# DPO’s Responsibilities

- Monitoring compliance with GDPR and data protection policies.
- Advising controller/processor concerning its GDPR's obligations.
- Training employees on GDPR compliance.
- Providing advice on data protection impact assessments and monitor their performance.
- Cooperating with supervisory authority.
- Involvement in and timely handling of all data protection issues or matters.

# Data Protection Impact Assessments

- Required when a processing activity is likely to result in a "high risk" to rights and freedoms of natural persons – specifically references when new technologies are implemented.
- Required for "large scale" processing activities involving special categories of sensitive  personal data.
- Required for automated processing activities that involve a "systematic and extensive evaluation of personal aspects relating to natural persons" which produce decisions having legal effects on a person.

# Data Protection Impact Assessments - Content

- Description of processing operations, purposes of the processing and, if applicable, the legitimate interests justifying the processing.
- Assessment of the necessity and proportionality of the processing in relation to the purposes served by the processing.
- Assessment of risks to the rights and freedoms of data subjects.
- Measures addressing the risks including safeguards, security measures and mechanisms to protect the data and to demonstrate compliance with the GDPR.
- Consultation with a supervisory authority is required if DPIA concludes an activity would result in "high risk" in the absence of measures taken by controller to mitigate risk.

# Cross Border Data Transfers (Adequacy Determination)

- Data protection mandated by the GDPR cannot be undermined by transfer of data outside the EU.
- Transfers permitted to a country with an adequacy determination – there are eleven (not the U.S.).
- No other specific approval or authorization required.
- U.S. Privacy Shield framework (self-certification process) approved by European Parliament and Swiss government.
- EU-U.S. Privacy Shield framework being challenged before Court of Justice of European  Union (Schrems II).

# Cross Border Data Transfers (Appropriate Safeguards)

- In the absence of an adequacy determination transfers are permitted if adequate safeguards are provided on the condition that enforceable rights and effective remedies for data subjects are available.
- Appropriate safeguards may be provided by:
  - Binding Corporate Rules.
  - Standard Data Protection Clauses.
  - Approved Codes of Conduct.
  - Approved Certification Mechanisms.
  - Standard Contractual Clauses between Controllers, Processors and/or data recipients.

# Cross Border Data Transfers (Derogations)

- In the absence of an adequacy determination or appropriate safeguards transfers may occur:

    1) With a data subjects' explicit consent.
    2) Necessary for performance of a contract between data subject and controller or to implement pre-contractual measures at data subjects request.
    3) Necessary to perform a contract concluded in the interest of the data subject between controller and another natural or legal person.
    4) Necessary for the establishment, exercise or defense of legal claims.
    5) Necessary to protect the vital interest of data subject or another person when data subject is incapable of providing consent
    6) Necessary for important public interests (recognized by Union or a Member State’s law).

# Cross Border Data Transfers

- Where no other basis or derogation exists, transfer is permitted if it's not repetitive, involves a limited number of data subjects, is necessary for a controller's "compelling" legitimate interest(s), which is/are not overridden by the interests or rights of the data subject, so long as the controller has assessed all of the circumstances surrounding the transfer and based on that assessment provided suitable safeguards for the data.
- Controllers and processors are required to document these assessments and safeguards.
- Authorizations approved and decisions adopted under Directive 95/46/EC remain valid until amended, repealed or replaced.
- Union or Member State law may set limits on transfers of specific categories of personal data outside the EU.

# Breach Notification – Supervisory Authorities

- Personal data breach, which triggers notification obligation, defined as a breach of security leading to an accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data.
- Personal data breach must be reported by a controller to relevant supervisory authorities, without undue delay and where feasible no later than 72 hours of learning of breach.
- Where notification is not made within 72 hours, it must include the reasons for the delay.
- Notification *not required* where breach is unlikely to result in risk to the rights and freedoms of natural persons

# Breach Notification - Data Subjects

- When a personal data breach results in a “high risk” to the rights and freedoms of natural persons, the controller must notify the affected persons.
- Notify without undue delay.
- Notification *not required* where the controller has implemented security measures that were applied to the involved data that renders it unintelligible (encryption) or has taken subsequent measure which ensure that high risk to data subjects’ rights and freedoms is not likely to materialize.
- If notification requires disproportionate effort notification should occur by public communication or by an equally effective means.

# Content of Breach Notices

- Description of the breach, and where possible the categories and approximate number of data subjects and personal data records involved.
- Name and contact information of the DPO or point of contact to obtain more information about the breach.
- The likely consequences of the breach.
- Measures taken or proposed to address the breach and to mitigated its possible adverse effects.
- Information may be provided in phases if impossible to provide all at the same time.
- Written in "clear and plain language."

# Breach Notification

- Processors are required to notify a controller of a personal data breach without undue delay after becoming aware of one.
- Controllers are required to document facts relating to a personal data breach, its effect and remedial actions taken (to enable the SA to verify compliance with its breach notification obligation).

# Data Protection By Design and Default

- At the time of determining the means of processing and at the time of processing, a controller shall implement appropriate technical and organizational measures designed to:
  - Implement data-protection principles such as data minimization, in an effective manner.
  - Integrate necessary safeguards into the processing in order to meet the GDPR's requirements and to protect the rights of data subjects.
  - Only process the personal data necessary for each specific purpose in terms of the amount of data collected, the extent of its processing, its retention period and the accessibility (must not be accessible by default to an indefinite number of persons).

# Questions?

# Thank You

**Steven M. Puiszis**

312-704-3243 I spuiszis@hinshawlaw.com

**www.hinshawlaw.com**