




GDPR Essentials

To Meet the May 25th Deadline

FIA Webinar – March 1, 2018



3/1/2018



Administrative Items

- The webinar will be recorded and posted to the FIA website following the conclusion of the live webinar.
- A question and answer period will conclude the presentation.
 - Please use the “question” function on your webinar control panel to ask a question to the moderator or speakers. Questions will be answered at the conclusion of the webinar.
- CLE certificates will be emailed shortly after conclusion of the webinar.



Upcoming Webinars and Events



Physical Commodity Trading – An Update on Developments in Regulation in the US, EU and UK

March 8, 2018 | 10:00 AM – 11:00 AM EST | Webinar



43rd Annual International Futures Industry Conference

March 13-16, 2018 | Boca Raton Resort & Club | Boca Raton, FL



40th Annual Law & Compliance Division Conference

May 2-4, 2018 | Omni Shoreham | Washington, DC

Learn more and register at [FIA.org/events](https://www.fia.org/events)



Today's Presenters

Michael Sorrell

Associate General Counsel, FIA

Melise Blakeslee

Partner, Sequel Technology & IP Law, PLLC
CEO, Achieved Compliance Solutions, LLC

Paula Bruening

Of Counsel, Sequel Technology & IP Law PLLC
Sr. Director, Global Privacy Policy, Achieved Compliance
Solutions, LLC



A Refresher on the Basics: the “*Big Changes*”

- *Policy shift from reliance on consent to accountability.*
- *GDPR is extraterritorial and applies to anyone offering goods or services to data subjects in the EU.*
- *Extremely broad definition of “personal data.”*
- *Required records of your processing.*
- *Must identify and maintain a legal basis for processing personal data. Consent is difficult to establish.*
- *Must honor the individual’s rights.*
- *Appoint a DPO and a Representative (not in every case)*
- *Direct responsibility for subcontractors and others*



Quick Review – Big Changes

Extraterritoriality

- Offering goods or services to data subjects in the EU.
- Or, monitoring their behavior.
- Residents of the EU are the beneficiaries. Nothing to do with citizenship. Expats in EU are also beneficiaries



Quick Review – Big Changes

Definition of Personal Data is entirely different that the old-style focus on name plus an account number, etc.

- “Any information related to an identified or identifiable natural person”
- A person’s business contact information is subject to all the GDPR protections. No distinction from “private life” data
- Safe to assume that all the data you collect must be treated in accordance with GDPR requirements



Quick Review – Big Changes

Record-keeping

- Article 30 requires written records of the data collected and purposes of processing. Data mapping is 1st step
- Where kept in all systems
- With whom is it shared
- Transfers to countries outside the EU
- US is not an “adequate” country. Result: data can only be transferred under approved mechanism
- Time limits on data retention
- Technical and security measures



Quick Review - Big Changes

Legal Basis for processing **MUST** be one of these:

- Consent (very difficult to establish, opt-out is dead, opt-in is dying)
- *Necessary* to performance of contract with *data subject*. Privity with data subject can be problem for FCMs
- Compliance with a legal obligation of controller (only EU legal obligations)
- Vital interests of data subject
- Public interest task
- Legitimate business interest weighed against interests of data subject



Quick Review – Big Changes

Honor individual's rights

- Right to be informed (who has the obligation to inform? Controller or processor?)
- Right of access
- Right of rectification and erasure
- Right of portability
- Need a process in place – 1/3 or UK residents plan on using their right to access data and request erasure.
- Rights don't always trump controller's right to retain information under certain circumstances – identify and write your playbook now.



Quick Review – Big Changes

Appoint a DPO

Appoint a Rep in the EU

- Not everyone needs to appoint a DPO, best practice may dictate
- DPO required if core activities consist of operations that require regular, systematic, monitoring of data subjects on a large scale
- Unless only occasional processing, then Rep is required if you do not have an establishment in the EU. (Data subject's convenience – not yours)
- Rep to maintain records, respond to data subjects, and regulators on all matters



Quick Review – Big Changes

Joint & several liability between controller, and all processors

- Law mandates contractual undertakings
- Actual management and oversight.
- Will require amendment of most contracts with 3rd parties who have access to personal data



Immediate steps (if not done already)

- Know your company's data.
- Know your company's vendors.
- Establish a policy that is accurate and promotes good privacy outcomes *for the data subjects*
- Appoint company staff in charge of data privacy oversight across the company.
- Begin workforce privacy training.
- Provide appropriate resources for security.
- Understand your company's needs for legal representation and support.



Know Your Data

- Conduct a review of your data holdings across the company
 - What does the company collect?
 - From where is the data collected?
 - With whom does the company share data?
 - How does the company process?
- Assess the risks data collection and processing raises for individuals.



Know Your Vendors

- GDPR holds companies responsible for protection and responsible use of their data no matter where or by whom it is processed.
- Liability for failing to protect data cannot be outsourced
- Companies must conduct due diligence to be sure vendors
- Have established good internal data protection measures
- Can meet the obligations that come with data
- Companies must clearly articulate data obligations in their contractual agreements.



Immediate Risk Reduction

- Make sure you have a written opinion about legal basis for processing: is it consent? Contract, legitimate business interest?
- Make sure privacy policy is accurate and transparent. Use data maps to ensure completeness.
- EU Cookie policy requirements
- Appoint staff to be responsible
- Have ready the documents regulators will require – Are you currently able to produce in 72 hours?
- Appoint a rep in the EU.
- Assess the risk data collection, storage and processing may raise to individuals, mitigate, and document the assessment.



On-going Risk Reduction

- Have a long-term plan, ensure regular management participation
- Breach remediation plan
- Breach notification plan
- Data transfer mechanisms
- Educate staff
- GDPR requires that companies implement technical and organizational security measure commensurate with the risk raised by processing data
- Companies must stay abreast of necessary software upgrades and patches
- Companies must be able to respond quickly to emerging threats.
- Data Retention and destruction
- Privacy by Design
- On-going risk assessments
- Obtain insurance



These are myths

- I can wait till May
- GDPR only applies to EU firms
- Consent solves everything
- GDPR compliance is primarily the IT department's problem
- I don't have to comply if we only collect business information
- I don't need a lawyer's help
- I have to isolate EU data
- Software solutions make me GDPR compliant
- I just need really good insurance
- I don't need to change my marketing practices
- My current privacy policy is good enough



Some industry specific problems

- How does customer consent intersect with obligations to obtain data, such as for anti-money laundering/financial suitability requirements?
- Obtaining consent through an intermediary, can it be done? Or, is direct privity required?
- When is consent mandatory?
- Officers and owners of entity customers - what is the obligation to provide notice?
- Is a code of conduct mandatory for a US FCM? How is this different from a GDPR compliance policy?
- How does a US FCM determine compliance with EU security standards?



Limits of Software-Only Solutions

Beware of claims that software or tools will make you GDPR compliant.

- Tools, generally, implement *mechanisms* of security or honoring rights, such as
 - Access controls
 - Data destruction
 - Encryption
 - Consent recording
 - Keep track of consents
 - Automate the individual's rights process, or
 - Help the DPO stay organised, track contracts
- Some, are diagnostic and help identify gaps in business processes, and track compliance, generate documents and records.
- Some educate



Melise R. Blakeslee, Esq.
Partner, Sequel Technology & IP Law, PLLC
CEO, Achieved Compliance LLC

Melise Blakeslee is the founding principal of Sequel Technology & IP Law, PLLC. Ms. Blakeslee has advised companies with respect to some of the largest databases in the world for financial transactions, clearing of travel, and media, as well as for many global membership organizations. A significant part of her practice relates to helping clients navigate the myriad number of international data protection laws, including breach crisis management.

In addition to her law practice, Ms. Blakeslee is the founder and CEO of Achieved Compliance Solutions, LLC offering an end-to-end privacy and data protection software solution for companies that are too understaffed and budget-constrained to effectively meet GDPR challenges. Her aim is to help business achieved GDPR-compliance in an efficient and cost-effective manner through the use of tools aimed specifically at those without the benefit of a dedicated privacy officer or staff.

Melise is a member of the International Association of Privacy Professionals, and the bars of New York and the District of Columbia. Prior to founding Sequel, Melise was a partner with a premier international law firm, heading its eCommerce and Technology department.

melise@sequeltechlaw.com
melise@achievedcompliance.com
571.366.1784

Paula Bruening
Senior Director, Global Privacy Policy

Paula brings 25 years of privacy and data protection policy development and representation expertise to her role at Achieved Compliance. Prior to coming to Achieved Compliance, Paula worked at Intel Corporation, where she was Director of Global Privacy Policy. At Intel she developed and coordinated data protection policy across the company, focusing particularly on the European Union.

Prior to her tenure at Intel, she served as Vice President for Global Policy at the Centre for Information Policy Leadership at Hunton & Williams LLP, a pathfinding privacy and information policy think tank located in Washington, D.C. addressing cross-border data flows, emerging technologies, and cyber security issues.

She was counsel for the Center for Democracy & Technology; Senior Attorney Advisor for the National Telecommunications and Information Administration of the Department of Commerce; and Senior Analyst for the U.S. Congress Office of Technology Assessment. Paula has extensive experience working on information policy issues in developing countries and with international organizations such as the Organization for Economic Cooperation and Development and APEC.

paula@achievedcompliance.com



Meet Achieved Compliance

ACHIEVED COMPLIANCE

Its suite of automated, software-based services combined with dedicated client counseling help companies quickly establish accountability-based data governance that responds to the requirements of regulators and the demands of the data-driven market. Using the PrivacyMinder software platform, and with the support of the Achieved Compliance legal team, budget-challenged companies can achieve the advantages enjoyed by larger industry players, but without the expensive outside counsel or consultants.

ACHIEVED REPRESENTATION SERVICES

The GDPR requires that U.S. businesses that collect data about European citizens maintain a registered representative in the EU. Our representation services provide on-the-ground EU presence companies need to comply with Article 27 of the GDPR. Located in the UK, Achieved Compliance Advocacy, Ltd. maintains required records, acts as a liaison to investigators and data subjects, as well as provides legal support in case of an investigation.

Achievedcompliance.com



FIA

