PlayWell, LLC

General Data Protection Regulation Overview

About PlayWell

- Data privacy and marketing compliance
  - Full-service compliance consulting: regulation, self-regulation and advocacy climates surrounding data privacy, policy development, training, product review and marketing
  - Expertise in education and entertainment technology
  - Create and implement organizational compliance practices and policies
  - 25+ years of compliance experience
  - Virtual CPO/DPO

PlayWell, LLC

What is the GDPR?

- Replaces the Data Protection Directive 95/46/EC
  - Harmonized data protection laws
  - Relied on DPAs' interpretations of the Regulation
  - Allowed transfer of personal data to third countries when the countries had guaranteed protection levels comparable to those in the EU
- Similar concepts in GDPR

GDPR – Quick Facts

- Effective May 25, 2018
- No “grace period” for compliance
- Regulation, not a directive
- Brexit will not impact implementation

Who Must Comply?

- Data controllers and processors in the EU
- Organizations outside the EU, offering goods or services, or monitoring behavior of individuals in the EU
- Processing personal data of data subjects residing in the EU

What Data is Impacted?

- Personal Data:
  - Any information relating to an identified or identifiable person, either directly or indirectly

Core Principles

Lawful, Fair, Transparent:

- Data is processed in a manner that is lawful, fair and transparent to the data subject
  - Obtain consent for each specific purpose prior to processing of personal data unless:
    - Processing is necessary for performance of a contract with the data subject
    - Processing is necessary for legitimate interests pursued by the controller or by a third party

Core Principles

Purpose Limitation:

- Data is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

Data Minimization:

- Data is adequate, relevant and limited to what is necessary for the purposes for which they are processed

Core Principles

Accuracy:

- Data is accurate; up to date; every reasonable step must be taken to ensure that personal data that are inaccurate are erased or corrected without delay

Storage Limitation:

- Data is kept in a form which permits identification of data subjects for no longer than necessary

Core Principles

Appropriate Security:

- Protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures

Costs of Non-Compliance

- "Effective, proportionate and dissuasive" fines
- Applied to the "undertaking"

  - Up to 10 000 000 EUR, or up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher
  - Up to 20 000 000 EUR, or up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher

Enforcement

- Each Member State will have an independent public authority responsible for monitoring application of the Regulation
  - Member States will enjoy cooperation in cross-border investigations

Key Roles and Responsibilities

Data Controller

- Determines purpose and means of processing personal data
  - Must “implement appropriate technical and organizational measures” to ensure compliance and demonstrate the measures they have in place
  - Liable for the actions of their processors

What Controllers Need

- Must ensure that data processors can and do comply with GDPR
- Record of processing activities
- Consider “with due regard to the state of the art,” if processors are able to fulfil their data protection obligations.

Data Processor

- Processes data on behalf of the controller
  - Must provide “sufficient guarantees” to meet the requirements of the GDPR
  - May process data only as instructed
  - Appropriate technical and organizational measures to comply
  - Prompt deletion or data return to the controller

Requirements

- Record-keeping
- Minimization
- Pseudonymization
- Transparency
- Auditing
- Enabling the controller to create and improve security features
- Policies and processes to ensure data protection by design and by default

GDPR in Action

Key Requirements

Auditing and Accountability:

- Must be able to demonstrate compliance with core principles
  - Audit, document, policies, procedures, accountability

- Written records documenting why, when and how compliance is achieved
- Data privacy by design and default
- Systems and data mapping

Key Requirements: Consent

- High standard of consent:
  - Freely given, specific, informed and unambiguous
  - Must have clear, written records demonstrating consent

  - Statement or a clear affirmative action
    - Not a precondition of use of the service
    - Not incentivized
    - Must allow for consent to be withdrawn

Key Requirement: Data Subject Rights

Withdraw consent - data erasure - data portability – object to processing for marketing and profiling

Benefit to the individual of sharing the data must outweigh the burden of sharing their data

Key Requirements: Data Security

- Evaluate and mitigate risks inherent in processing with an appropriate level of confidentiality and security

Take into account “the state of the art” and costs of implementation in relation to risks and nature of the personal data to be protected

Key Requirements: Breach Notification

- Controller must notify the supervisory authority of a breach without undue delay and, where feasible, not later than 72 hours after having become aware of it
  - Where that can't be achieved, it must be accompanied by a reason

Data Transfer Outside of the EU

- Make use of binding, enforceable corporate rules
- Contract requirements:
  - Standard data protection requirements
  - Delete or return all personal data after the services are provided
  - Specify information to demonstrate compliance with GDPR; allow for audits and inspections

Key Requirements: Data Protection by Design and Default

- Privacy by Design:
  - Implement appropriate technical and organizational measures taking into account the protection of the data for the lifecycle of the product
- Privacy by Default:
  - The strictest privacy settings automatically apply

Key Requirements: Data Protection Officer (DPO)

- Must be appointed for:
  - Public authorities
  - Organizations that engage in large scale systematic monitoring
  - Organizations that engage in large scale processing of sensitive personal data
- Specific expertise, reporting structure and responsibilities

Questions?

PlayWell, LLC

Compliance Consulting

Linnette Attai, President & Founder

Linnette@PlayWell-LLC.com +1 917-485-0353

www.PlayWell-LLC.com Facebook.com/PlayWellLLC @PlayWell_LLC