GDPR:
The Seismic Shift in Marketing Analytics

Evan Levy
Vice President, Data Management Services
May 16, 2018

Agenda

- Data Privacy and Protection Concepts
  - Real World Privacy Issues
  - Privacy and Protection Fundamentals
- An Overview of GDPR
  - Requirements Overview
  - 5 Basic Steps for GDPR Compliance
- Q & A

133EC8F

Disclaimer

The content provided within this presentation (referred to as “The Information”) is for informational purposes only and does not constitute legal advice. The Information should be used as guidance and modified to meet your requirements and the use of and reliance on The Information is at your sole risk.

The Information available within this presentation is provided without any warranty, express or implied, including as to its legal effect and completeness. We make no claims, promises, or guarantees about the accuracy, completeness, or adequacy of The Information and assume no duty of care to any person in respect of The Information and its contents. We expressly exclude and disclaim liability for any cost, expense, loss or damage suffered or incurred in reliance on The Information or it meeting your needs, including (without limitation) as a result of misstatements, errors and omissions in their contents.

133EC8F

Data Breaches

“In October, 2017, Yahoo acknowledged 3 billion user accounts had been compromised due to hackers dating back to 2013”

“In July, 2017, a data breach at Equifax exposed personal information on 143MM consumers”

“In September, 2014, Home Depot admitted that hackers gained access to 56MM debit and credit card records”

“In November, 2017, Uber disclosed hackers got the names and driver’s license numbers of 600k drivers and personal data on 57MM Uber users in late 2016”

133EC8F

Data Protection Neglect

"In the state of California, 19.2 Million voter records were stored in an unsecured database (July, 2017)"

"In July, 2017, World Wrestling Entertainment exposed personal information on 3 Million customers in an unprotected cloud database"

"In July, 2017, 14 million Verizon customer records were found unsecured on an Amazon storage server controlled by Israeli-based Nice Systems"

"In June, 2017, The Republican National Committee failed to secure a server which contained the personal information of 198 MM voters"

133EC8F

Data Liability Costs

"In 2015, AT&T agreed to pay a $25MM fine for privacy violations related to a 2014 breach that exposed almost 280,000 customers personal information"

"In March, 2017, Honda was fined $104k for sending marketing emails to people without the appropriate consent"

"In In 2013, the makers of a social networking application called Path were fined $800k for collecting personal information from children without parental consent"

"In October, 2014, the FCC fined two telco carriers $10MM for storing customer PII data online without adequate security safeguards"

133EC8F

What is Data Protection?

The safeguarding of the privacy rights of individuals in relation to the processing of their personal data

Comhairle Contae Thiobraid Árann
Tipperary County Council

…legal safeguards to prevent misuse of information stored on computers, particularly information about individual people..

Encarta

…laws and regulations that make it illegal to store or share some types of information about people without their knowledge or permission.

Cambridge Dictionary

The process of protecting data involves the relationship between the collection and dissemination of data and technology, the public perception and expectation of privacy and the political and legal underpinnings…

techopedia

133ECF2

sas

Data Privacy and Protection Concepts

sas

sas

Data Protection

The adoption of administrative, technical, or physical deterrents to safeguard data. Ensuring data is used for only approved processes.

Ensuring that data is safe from…

- Data corruption or catastrophic events
- Unauthorized or illegal access
- Data loss or unplanned deletion
- Inappropriate (or illegal) processing or usage
- Misuse
- Being stored without necessary protection

133ECF2

Personally Identifiable Information (PII)

PII Any information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means

Demographic Data
- Name
- Home Address
- Home Phone Number
- Mobile Phone Number
- Email Address
- Date of Birth

Government IDs
- Passport Number
- Social Security Number
- Vehicle Registration ID
- Driver License

Bank /Card Accounts

Sensitive Data
- Health
- Sex
- Political
- Religious
- Philosophical
- Trade union
- Genetic
- Biometric
- Race
- Gender
- Ethnicity
- Children

Employment
- Employer
- Employment ID
- Work Address
- Work Phone Number

Digital Identifiers
- IP Address (V4, V6)
- MAC Address
- Long/Lat Location
- Twitter Account
- URL Facebook
- URL LinkedIn

133ECF0

Controllers vs. Processors

The data controller must exercise control over processing – they are responsible for its data protection. They determine the purpose for which data are processed.

The data processor processes data on behalf of the data controller.

Controller

- Acquire and collect personal data
- Identify purpose the data is to be used
- Decide whether to disclose the data's existence (and to whom)
- Decide whether individuals' rights apply
- Identify data retention period

Processor

- Establish methods to collect and store the data
- Define security implementation method
- Identify means to transfer data between parties
- Identify methods for adhering to the retention schedule
- Determine method to dispose of the data

133ECF0

Data Anonymization

The process of either encrypting or removing personally identifiable information from data sets, so that the people whom the data describe remain anonymous

Original Data

Customer ID	30391244
First Name	Bob
Middle Name	James
Last Name	Smith
Birthdate	04/12/1939
Street Address	123 S Oak Street
City	Ava
State	Ill
Postal Code	62907

Different Methods for Anonymization

00000000	1318870	B3D0AD9
XXXX	Vydvq	408B933
XXXX	Majes	47A26CAD
XXXXX	Oikyf	0049C4DE
00/00/00	03/12/1940	26CADF9D
XXX XXXXX	432 Siocy DC	AD200442
XXXXXX	Fiyt	3D0A2000F
XXX	XU	D20ED049C
00000	45829	043469C40

- There are numerous methods for data anonymization (encryption, hashing, pseudonymization, etc.)
- Anonymization irreversibly destroys any way of identifying the data subject

133ECF0

Types of Data Consent

Data Consent — Permission to use and process personal data in a manner different from the original purpose that the data was collected and used.

Data Collection

Data Usage (processing)

Data Sharing

Data Retention

Laws that address consent vary by country and in most instances by industry

Traceability, Tracking, Lineage

Traceability — The ability to verify the history, location, or application of an item by means of documented recorded detail

History of data value

- Change history
  - Date of creation to current day
  - All Values
  - System-to-system movement

Tracking all copies

- Location of PII data copies within company
- Location of PII data sent to external parties
- Specific PII elements and their values (copied)

Responsible party

- "Hands-on" individual responsible for tracking
- CISO within company
- Location of details

Who has access

- Who has used the data
- How is the data accessible
- How is it shared
- How is it secured

Data Deletion

PII data deletion is the purging and removal of PII data for a specific individual.

- Deletion is not “removing access” or “labeling data to make it unavailable”
- Deletion is the purging and removal of the data content
- Deletion also requires that a process is in place to ensure offline archives are purged or processed in a manner to ensure that data is not retained

There are numerous issues associated with this…

- There are no laws requiring deletion if a company must address existing business obligations (payment processing, warranty, etc.)
- Data Deletion is not a uniform requirement across the world
  - There are numerous states and countries that require internet data deletion
  - Specific details vary by governing body, industry, and subject area content

133ECF2

Data Protection Concepts

Data Protection methods and practices will vary based on the “state” of data, the user audience, and type of processing and usage

Protecting Data
-- When Processing --

- Controlled by OLTP application
- Access limited to specific programs
- Gathered for specific business function
- Usage limited to specific purpose
- Access is limited; data protected in storage (not in program memory)

Protecting Data
-- When Stored --

- Raw content is rarely protected; access is controlled (DBMS, file access)
- Access exists for sharing
- Made available to support new, different purposes
- Usage responsibilities, limitations rarely defined

Protecting Data
-- In Movement --

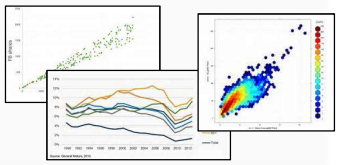
- Most programmatic movement is highly protected (APIs, WebSvcs, etc.)
- Manual movement tends to ignore protection (email, ftp, etc.)
- Production movement is often reviewed and approved
- Manual movement and sharing is error-prone

133ECF0

GDPR Overview

Are You Affected by GDPR?

Analyzing consumer data to understand behavior



Use 3rd party data to market to prospective customer (consumer)

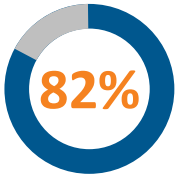
Ship customer data to 3rd party for promotional purposes

Review customer purchase history for customer support inquiry

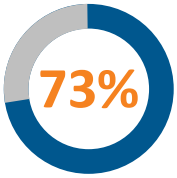
You have EU resident data, but don't conduct business in EU

133C8A5

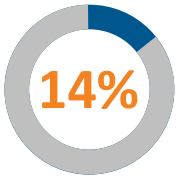
GDPR Compliance Remains a Challenge



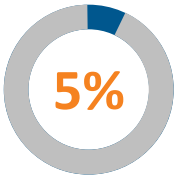
Consider GDPR will affect their business



Fear to lose confidence from customers in not being compliant



Consider they understand GDPR



Are taking the necessary steps to prepare for GDPR

Source: SAS Institute, May 2017

EU General Data Protection Regulation (GDPR)

What's it About?

- The reform strengthens citizens' fundamental rights in the Digital Market and focuses on Personal Data
- GDPR repositions ownership of personal data to the individual
- "Data possession" is no longer the same as "data ownership"
- The Regulation was put into place 24 May 2016; penalties apply starting 25 May 2018
- The Regulation promotes techniques such as anonymization (removing PD), pseudonymization (replacing PD), and encryption (encoding PD)

- Sanctions: Up to €20 MM or up to 4% of the worldwide revenue (whichever is greater)

http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm

133C8A5

How GDPR Impacts non-EU based Organizations

Applies to companies processing EU resident data

- Independent of business transaction location
- Based on where consumer resides

Organizations must take “appropriate” measures to demonstrate compliance…

- Data inventorying and record-keeping of all EU personal data that is processed
- Data breach notification to regulators and individuals
- The right to be forgotten (request personal data be erased)
- Routine Privacy Impact Assessments
- Mandatory appointment of data protection officers (DPOs)
- Individuals right of Data Portability

133C8A5

The Challenges of Data Protection & Privacy

Towards Authorities

Can we produce a list of all of PII data that’s stored

Do we have an overview of all data sources?

Is the data protected?

Do we know who has access to the data

Can we show that processes exist to protect the data

Internal Challenges

What is Personal Identifiable Information (PII)?

What if DQ issues make identification impractical

Do we control (and log) all access?

Do we have universal adoption?

Who tracks and measures conformance ?

133ECF2

GDPR

Core PDP/Privacy Activities

GDPR contains 99 articles (regulations) covering a wide variety of protection and privacy details

GDPR Articles

Define PII Data Element

Article 4: "'Personal data' means any information relating to an identifiable natural person

Article 15: "The data subject shall have the right to obtain from the controller…a copy of the personal data undergoing processing"

Article 4: "a person is one who can be identified…by reference to an identifier such as a name, an identification number, location data, an online identifier…"

Define PII Elements

Article 16: "The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her."

Article 9: "Processing of data revealing racial or ethnic origin, political opinions, religious beliefs…for the purpose of identifying a person…shall be prohibited."

Article 17: "The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay"

133C8FA

** Article text summarized for clarity and readability*

Define PII Elements: Actions to Take

Identify company PII data glossary

Productionalize data correction

Evaluate each system's need for PII data

- Establish "the list" of PII data elements
  - Start with the standard, company-independent elements
  - Identify company-specific elements (e.g. account number, equipment address, etc.)
- Expect to "spin-up" a review process that evaluates systems maintaining their own copy of PII data

133C8A5

GDPR Articles

Identify Sources

*Article 5:"*Personal data shall be …limited to what is necessary for purposes for which they are processed."

Article 14: "Where personal data has not been obtained from the data subject, the controller shall provide …the period for which the personal data will be stored…"

Identify Systems

Article 5: "…collected for specified purposes and not further processed in an manner that is incompatible with those purposes"

Article 25 : "Controller shall implement appropriate measures for ensuring that only personal data which is necessary for each specific purpose of the processing are processed."

Article 5: "…processed in a manner that ensures appropriate security …"

Article 32: "Processor and any person ... who has access to personal data shall not process them except on instructions from the controller"

133C8FA

** Article text summarized for clarity and readability*

Identify Sources : Actions to Take

Conduct data discovery to identify existing data sources

Inventory data content; ID primary / secondary copies

Establish primary source "System of Record"

- Inventory and identify the different Customer PII data sources
  - The focus must be content, not column or field names
  - Consider both data processing systems and repositories
- Differentiate the "System of Record" from unmanaged copies
- Develop method to evaluate all new/emerging systems

133C8A5

GDPR Articles

Governance Details

Article 7: Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data."

Article 18: "… The data subject shall have the right to obtain from the controller restriction of processing where the accuracy of the personal data is contested by the data subject

Article 13: "When data is collected, the controller shall provide: the purposes of processing; the period stored; contact details of the DPO; the right to correct; the right to erase; …"

Governance

Article 23: "…law may restrict the scope of [individual rights]…to safeguard…national security, defense, public security…"

Article 30: "Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility."

Article 28: "Processing by a processor shall be governed by … law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing"

133C8FA

** Article text summarized for clarity and readability*

Governance: Actions to Take

Align GDPR with data governance program

Establish process for deployment (and a adoption)

Identify monitoring (& enforcement) bodies

- Position GDPR activities to align with corporate data governance effort
  - Don't position GDPR as a separate governance initiative (adoption and enforcement requires enterprise level authority)
  - Ensure that Data Governance body has responsibility to monitor deployment and adoption of all policies, rules and mechanisms
- Expect to grow investment in Data Governance

133C8A5

GDPR Articles

Protect Details

Article 24 "the controller shall implement appropriate …measures to ensure and to demonstrate that processing is performed in accordance with this Regulation"

Article 32: "..the processor shall implement appropriate…measures to ensure a level of security appropriate to the risk including…the pseudonymization and encryption of personal data …"

Article 25 "…controller shall implement appropriate technical and organizational measures… in order to …protect the rights of data subjects."

Protection Methods

Article 32 "The controller and processor shall ensure that any person acting under authority…who has access to personal data does not process them except on instructions from the controller"

Article 34 "The communication to the data subject … shall not be required if… data affected by the personal data breach, in particular those that render the data unintelligible to any person who is not authorized to access it, such as encryption …"

133C8FA

** Article text summarized for clarity and readability*

Protect: Actions to Take

Determine data protection approach for all PII elements

Establish protection standards for static and moving data

Establish measurement / monitoring mechanisms

- Establish/Centralize customer data security into single chain of authority
  - DPO will need to coordinate with CDO, Data Governance Program, and various IT development and maintenance teams
  - Establish data security "checks & balances" (compliance, business needs, usability)
- Establish and socialize "Data Usage Responsibilities"

133C8A5

GDPR Details

Measure & Audit

Article 32: "…a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing…"

Article 33: "…In the case of a data breach, the controller shall notify the supervisory authority within 72 hours after having become aware of it…"

Measure & Audit

Article 39: "The DPO will monitor compliance … to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff…;

Article 40: "A code of …shall contain mechanisms which enable the body …to carry out the mandatory monitoring of compliance"

Article 35: "When implementing new technologies… the controller shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data."

133C8FA

** Article text summarized for clarity and readability*

Measure & Audit: Actions to Take

Identify owner and budget for audit publishing

Identify GDPR KPIs and metrics to publish

Establish process to review all new applications (and data)

- Develop plan to monitor and log PII data access and usage
  - GDPR establishes DPO as owner of audit activities
  - Leverage experience from production support and security monitoring areas
- Establish review process for GDPR compliance for all new applications and data (prior to deployment)

133C8A5

Other Government PDP Initiatives

More than 50 countries have enacted data privacy laws focused on the private sector and reestablish data rights, ownership, and possession responsibilities.

Many countries have multiple laws governing various aspects of personal information.

Mexico	The Federal Law on the Protection of Personal Data held by Private Parties (Ley Federal de Protección de Datos Personales en Posesión de los Particulares)
Canada	Personal Information Protection and Electronic Documents Act (PIPEDA). The Privacy Act.
England	Data Protection Act
Australia	The Privacy Act of 1988; Australian Privacy Principles (2014)
Singapore	Data Protection Act 2012 (PDPA) – and currently in the midst of a revision
India	Information Technology Act, 2000. Information Technology (Amendment) Act, 2008
Japan	Act on the Protection of Personal Information (APPI)

What We're Telling Our Clients…

GDPR isn't a separate initiative –it's part of a data strategy

- PII and PDP isn't limited to reporting and data delivery
- GDPR requires a coordinated approach across multiple data management disciplines

Deploying GDPR isn't a "once and done" project

- Data protection and security will continue to evolve (and expand)
- PDP and PII must become integral to data usage, sharing, and development

An active Data Governance program is crucial to GDPR success

- GDPR isn't a stand-alone activity; Data Governance should manage and drive GDPR adoption

133C713

Thanks!

Evan Levy
VP, Data Management Services
Evan.Levy@sas.com

@EvanJayLevy

sas.com

THE POWER TO KNOW.