Risk Management and the GDPR: Interpretations and Implications

April 1, 2019

Ann Jordan
General Counsel, ASQ

ASQ
The Global Voice of Quality®

Today’s Journey

- Welcome to the Digital Era
- GDPR Review
- Month 10 takeaways
- CCPA and beyond
- Data breach and US litigation

Welcome to the Digital Era

- As of January 2019, the digital population hit 4.4 billion (Statistica)
- Approximately 2.5 quintillion of data are created each day (DOMO)
- By 2020, it's estimated that 1.7 megabytes of data will be created per second, per person (Forbes)
- In 2018, 89% of organizations had plans to adopt or had already adopted a digital-first business strategy with Services (95%), Financial Services (93%) and Healthcare (92%) leading all industries (IDG)
- Data driven organizations are 23x more likely to acquire customers, 6x likely to retain customers and 19x more likely to improve ROI (McKinsey Global Institute)

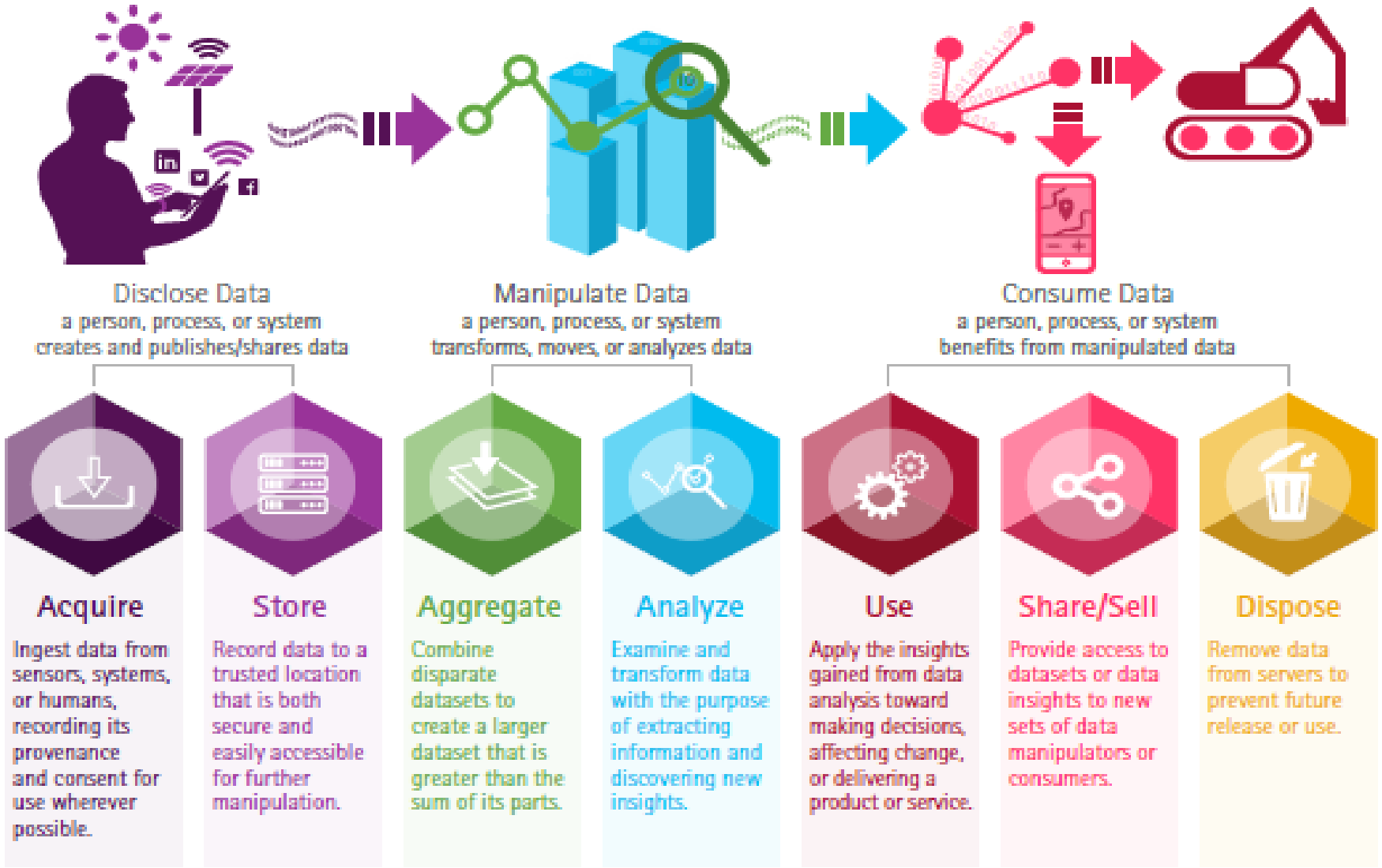
ASQ

Welcome to the Digital Era

- The digital economy is built on data – massive streams of data being created, collected, combined, analyzed and shared – for which traditional governance frameworks and risk-mitigation strategies are insufficient.

- How organizations handle data throughout the supply chain can have a decisive impact on their reputation, effectiveness and continued existence.

Data Supply Chain (Accenture)



Welcome to the Digital Era

Implication: Digital era laws and regulations related to data supply chains mandate Quality applications and heightened risk management

GDPR Overview

ASQ®

Concepts:
Privacy v. Data Security

Privacy: Focus on rules governing acts that PUSH personal information out of an organization, typically in connection with acquisition or retention of customers

Data Security: Focus on rules aimed at protecting personal information from being PULLED out of an organization

The GDPR collapses both concepts under the rubric of DATA PROTECTION

GDPR Overview

Effective Date:
May 25, 2018

Territorial Scope:

- Organizations established in the EU that process personal data (even if processing is outside the EU)
- Organizations outside the EU but that offer goods and services to EU data subjects or monitor the behavior of data subjects in the EU

GDPR Overview

Penalties:

- Fines up to $20M euros or 4% of worldwide revenue from the prior year (whichever is higher)

Protections:

- Places safeguards on, and requires CONSENT for, the use or PROCESSING of an individual's PERSONAL DATA

Responsibilities:

- For PROCESSORS and CONTROLLERS of personal data

GDPR Key Terms

What is PERSONAL DATA?

- "Any information related to an identified or identifiable natural person."
- No definitive list; circumstantial
- Includes emails, cookies, device IDs, images, recordings, phone numbers, SSNs, addresses and other online identifiers

What constitutes CONSENT?

- Freely given, specific, informed and unambiguous
- Must be revocable
- Presumption that consent will not be valid unless separate consents are obtained for different processing activities
- General, omnibus consent will not be valid
- Burden of proof rests with the controller

GDPR Key Terms

What is PROCESSING?

- Any operation or set of operations performed on personal data or sets of personal data, whether or not by automated means, such as 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.

What is a CONTROLLER?

- An entity that alone or jointly with others determines the purposes or means of the processing of personal data

What is PROCESSOR?

- An entity that processes personal data on behalf of a controller

ASQ

GDPR Processing Security

Art. 32 describes the appropriate level of security for processing personal data:

- “Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.”

GDPR Processing Security

GDPR requirements go beyond security in the classical sense and include concepts of availability and reliability

Security controls should take into account:

- Cost of implementation
- Nature, scope, context, purpose of processing
- Risks to data subject in the event of breach

GDPR Processing Security

Required technical and organizational information security measures include:

- Pseudonymization and encryption of personal data
- Ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services
- Ability to restore access to personal data in the event of a physical or technical incident
- Regularly testing, assessing and evaluating the information security program

GDPR Processing Security

- Mandates risk assessments
- In classical risk analysis in information security, risks traditionally focus on potential damage to the organization. GDPR risk assessment depends on the impact to the to the data subject.
- Likelihood also must account for internal and external

The level of data protection risk can be calculated as:

Risk level for the rights and freedoms of data subjects	=	likelihood	×	severity (=potential damage)

Comparison of the Requirements of DIN ISO/IEC 27001:2015 and GDPR

Phase in an ISMS	Article 32(1)(2) of the GDPR
risk assessment appropriate technical and organizational measures are to be taken incorporates: ▪ state of the art ▪ implementation costs ▪ nature, scope, context and purposes of the processing assessment standard (objectives): ▪ confidentiality ▪ integrity ▪ availability	"Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk." (Article 32(1)(1) of the GDPR) "In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed." (Article 32(2) of the GDPR)
A catalog of measures has to be developed, which meets at least the following criteria ▪ pseudonymization ▪ encryption ▪ confidentiality ▪ integrity ▪ availability ▪ fast BCM	"these measures include inter alia as appropriate": a) the pseudonymization and encryption of personal data b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident (Article 32(1)(2)(a-c) of the GDPR)
internal audits and management review and Procedures for correction / adaptation of measures taken	"these measures include inter alia as appropriate": a) "a procedure for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing" (Article 32(1)(2)(d) GDPR)

GDPR Rights of Data Subjects

GDPR Rights of Data Subjects

Right to be forgotten

- Personal data must be erased without undue delay when:
  - Retention is not required
  - Data is no longer needed
  - Consent has been revoked

Data portability

- Individuals must be given the right to transfer data to another service provider where technically feasible

GDPR Rights of Data Subjects

Right to be informed

- Privacy Notices
- Transparency about how data is used

Right of access

- Individuals are entitled to see the personal data your organization holds about them
- One month to comply with the request at no fee (unless request is manifestly unfounded or excessive, particularly if it is repetitive)

ASQ

GDPR Rights of Data Subjects

Right to rectification

- Individuals are entitled to have personal data rectified if it is inaccurate or incomplete.

Right to restrict processing

- Individuals have a right to ‘block’ or suppress processing of personal data.

Right to object

- Individuals can object to certain data processing.

ASQ

Overview of Data Collection Requirements

When personal data is collected from a data subject, the following information must be provided:

1. Identity and contact details for controller
2. Contact details for DPO
3. Purpose of processing
4. Legitimate interests
5. Recipients of the personal data
6. Transfer of data to third countries
7. Data retention periods
8. Other data subjects rights

ASQ

GDPR Security Breach

Breach Notification

- Definition: “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed”
- Controllers must notify supervisory authorities, and in turn data subjects, within 72 hours of becoming aware of a data breach
- Notice not required if “the personal data breach is unlikely to result in a risk for the rights and freedoms of data subjects”
- Controllers must document all breaches including the facts, effects and remedial actions

ASQ

GDPR Preventative Measures

Privacy by design

- Proactive approach
- Personal data protection mechanisms must be built at inception for product development, software development, IT systems, etc.

Data protection impact assessments (DPIAs)

- Required for new technologies
- Required when processing is likely to result in a high risk to the rights and freedoms of individuals.

GDPR 10 months in…

- DPAs are overwhelmed (up to a 1200% increase in complaint and breach and notifications)
- Data processing agreements and the emergence of market positions
- EDBP guidance, including extraterritorial transfers
- E-privacy
- Enforcement actions commenced from various supervisory authorities

ASQ

GDPR Enforcements

- Enforcement actions have been specific in focus
- Nonprofits on the offensive
- Encryption of passwords
- Cooperation reduces fines
- France leads the way
- Google lessons learned: (a) one-stop shop won't save you and (b) form matters as much as substance

Google fined 50 million Euros in France over GDPR failures

Mirror Posted On: 22nd Jan 2019 08:30:00 GMT +0200

Google has been fined for not having "legal basis" for processing personal data in France. (Photo: Mirror)

Google has been given a 50 million Euro fine in France over data protection failures, particularly focusing on how it processed personal data for advertising services.

Additional Laws and Regulations

Other privacy/breach foreign laws:

- Australia, Israel, Brazil, Canada, China (criminal) and Japan

US:

- Data breach laws in all 50 states
- 11 state privacy bills are under consideration
- 4 federal privacy bills have been introduced but have not received momentum
- CCPA
- Proposed Washington state privacy act most resembles the GDPR (including risk assessments)

ASQ

The California Consumer Protection Act

ASQ

CCPA

Effective January 2020

- Political inception (ballot initiative replacement)
- Ruling making by July 2020

Consumer Rights

- Knowledge of what personal information is being collected
- Access to personal information and business practices
- Deletion of personal information
- Opt-out of sales of personal information
- Anti-discrimination for exercising rights

Excludes

- Aggregate or de-identified personal information
- Conduct wholly outside California

Implementation Requirements

AG Enforcement and Private Right of Action

Scope of CCPA

Any company that does business in California and meets one or more of these standards:

- Annual gross revenue over $25 million
- Collects or shares personal information annually from 50,000 consumers, households, or devices
- Derives at least 50% of annual revenue from sale of personal information

Obligations and limitations extend to all **personal information** maintained about **consumers**.

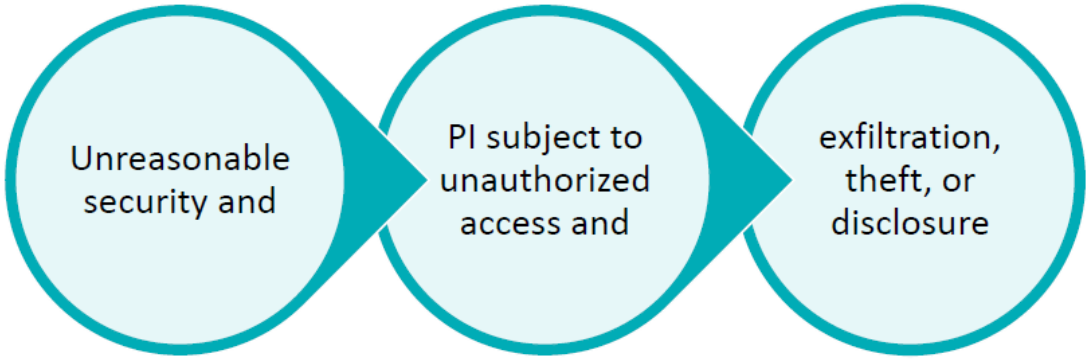
- Consumer = any natural person who is a California resident
- Personal Information = information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked with consumer or household

***The CCPA PI definition includes 11 broad categories of personal information

ASQ

CCPA

Private Right of Action



Encryption and redaction exception

Different definition of personal information for this section, limited to individual's first name/initial, plus last name, plus:

Social security number	**Driver's license or state identification card number**	**Financial account number, credit or debit card number in combination with access code**	**Medical information**	**Health insurance information**

Currently applies to a failure by the "business" to implement and maintain reasonable security.

ASQ®

Data Breach and US Litigation

ASQ

Breach by the Numbers

Over

53,000

security incidents and

2,200

breaches reported in 2017*

(2018 Verizon Data Breach Report)

27%

discovered by third parties

56%

caused by a third party

- US average cost for a data breach in 2017 was $7.91M
  (“Global Overview” from IBM Security and Ponemon Institute)
- Cybercrime resulted in a $600B loss to the 2017 global economy
  (McAfee and the Center for Strategic and International Studies)

ASQ

What is a Duty of Care?

- If you are breached and your case goes to litigation, the court will determine whether you had and satisfied a “duty of care”
- The legal concepts of a “duty of care” requires that organizations demonstrate they used safeguard to ensure that risk was reasonable to the organization and appropriate to other interested parties at the time of the breach
- Multi-factor test
- Less than due care = negligence = liability
- A current gap exists between information security risk assessments and litigation expectations

ASQ

What Courts Mean by Reasonable Safeguards

Safeguards should not be more burdensome than the risks they protect against

- The risk must look beyond the asset
- Consider foreseeable threats, their likelihood and impact, the reason the risk is engaged, and the burden of alternative safeguards

Find the balance between what you *should* do to protect others, and what you *can* do as a business.

Why are Current Risk Assessments Failing with the Courts?

- No risk appetite statement
- Key personnel not involved
- Only considers the organization's risk (not public/customer)
- Quantifies risk only in terms of dollar limits
- Lacking key insights and implications leaving decision makers not knowing what to do next and how it may impact business plans and decisions
- Difficult to measure probability/likelihood

Current Security Assessments (Halock)

	Evaluates Risk to Info Assets						Evaluates Due Care		
Method	**Standard of Care**	**Identifies Vulnerabilities**	**Considers Threats**	**Evaluates Harm to Self**	**Evaluates Harm to Others**	**Estimates Likelihood**	**Defines Acceptable Risk**	**Defines Reasonable**	**Evaluates Safeguard Risk**
DoCRA CIS RAM	●	●	●	●	●	●	●	●	●
IT Risk Assess ISO 27005, MIST SP 800-30, RISK IT	●	●	●	●	○	●			○
FAIR Factor Analysis for Info Risk		●	●	●		●			
Gap Assessments Audits, Y/N/P	●	○							
Maturity Model Assessments CMMI, HITRUST, FFIEC CAT	●								

Duty of Care Risk Scoring for Impact

Identify the following to prepare risk criteria:

- Your *mission*: what you do for the world
- Your *objectives*: what you do for yourself
- Your *obligations*: the care you owe others

Multiple Impact Categories	Customer Performance (Mission)	Profitability (Objective)	Protection PI (Obligations)

What Judges Will Ask After a Breach (in plain language)

- Was the breach foreseeable?
- Did you consider the impact of the harm the breach could have caused?
- What did the public and injured parties gain by you engaging in the risk?
- What benefit did you gain from engaging in the risk that lead to the breach?
- What alternative safeguards would have mitigated the risk?
- Would those alternative safeguards have imposed an undue burden on you?
- How well would these alternative safeguards have reduced the risk of harm (impact)?
- Would the proposed safeguards have created other undesirable risks?

ASQ

Questions?

ASQ®
The Global Voice of Quality®