EUROPEAN UNION'S GENERAL DATA PROTECTION REGULATION ("GDPR")

Capital Region Business Presentation
April 16, 2019

Fred J. M. Price
fjprice@bsk.com
Syracuse, NY
(315) 218-8130

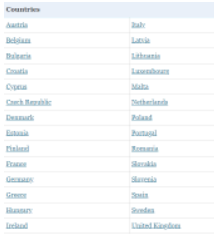
GDPR Background

- European Union regulation to streamline and unify data protection laws across Europe.
- Effective May 25, 2018.
- The right to protection of "personal data" is considered a fundamental right comparable to US Bill of Rights.
- Places certain restrictions, and imposes certain obligations, with respect to the "processing" of personal data.

2

GDPR Background

- The GDPR gives individuals whose "personal information" is being "processed" certain rights and protections relative to that information.
- The GDPR may apply to entities located wholly outside of the EU, depending on how entities collect and process personal information.
- EU Member States
  - *EEA Member States
    - Norway, Iceland, Liechtenstein



Countries	
Austria	Italy
Belgium	Latvia
Bulgaria	Lithuania
Croatia	Luxembourg
Cyprus	Malta
Czech Republic	Netherlands
Denmark	Poland
Estonia	Portugal
Finland	Romania
France	Slovakia
Germany	Slovenia
Greece	Spain
Hungary	Sweden
Ireland	United Kingdom

What is Personal Information?

- Personal Information/Data is **any** information relating to an individual, whether it relates to his or her private, professional, or public life **that can directly or indirectly identify the individual.**

- Name
- Home address
- Photos
- Email address
- Bank details
- Posts on social networking websites
- Medical information
- IP address
- Subsets of particularly sensitive Personal Data:
  - "Special categories"
  - Children's Personal Data
  - Criminal records.

What is Processing?

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

- collection
- recording
- organization
- structuring
- storage
- alteration
- adaption
- retrieval
- consultation
- use
- disclosure by transmission
- dissemination or otherwise making available
- restriction
- erasure
- destruction

Controller/Processor

- Controller of Personal Data
  - *the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the **processing** of personal data*
  - Responsible for compliance of Processor

- Processor of Personal Data
  - *a natural or legal person, public authority, agency or other body which **processes** personal data on behalf of the controller*
  - Sub processors
  - Report to Controller

Application to US Businesses

- Processing of Personal Data
- Scope: GDPR applies anywhere if…..
  - **Establishment test**: personal data controlled or processed by an entity established within the EU
  - **Bellybutton test**: personal data about a person located in the EU (regardless of citizenship)
  - **Transfer test**: personal data transferred outside of the EU
    - If so, need adequate level of protection/safeguards
      - Binding corporate rules
      - Standard contract clauses
      - EU-US Privacy Shield

Application to US Businesses

- Brick and mortar operations in EU.
- Employees physically located in the EU.
- Online sales into the EU.
- Targeted *offering* of goods/services in the EU.
  - e.g., do marketing materials/website display:
    - EU countries, languages or currencies
    - contact information reachable from an EU country
    - list international customers or distributors
    - "we deliver goods" or "offer services" in EU

8

Application to US Businesses

- Monitor EU data subjects - collection and subsequent reuse of the relevant data about an individual's behavior within the EU
  - e.g., cookies, geolocation tracking
- Personal data transfer into/out of EU
  - e.g., for cloud storage directly or through a vendor in the EEA per contract
- GDPR is not implicated for certain business-to-business processing (e.g., invoice without personal data)

9

Compliance: 6 Principles of Processing

1. Processed **lawfully**, fairly and transparently.
2. Processed for specified, explicit and legitimate purposes.
3. Adequate, relevant and proportionate or limited to the information necessary for the purpose.
4. Be accurate and current.
5. Retained only as long as necessary.
6. Processed securely using "appropriate technical or organizational measures."

- *Controllers required to demonstrate compliance.

Lawful Bases for Processing

- Consent.
- Necessary to perform contract.
- Required by law (this refers to applicable EU law, not US law).
- "Legitimate interests"
- Necessary for vital interests/Data Subject incapacitated.
- Necessary to perform a task in the public interest (again, this is per EU-focused public interest, not US).

- Must document bases!

Misconception Alert - CONSENT

- A common misconception is that consent is required in order to collect Personal Data.
  - "Consent" of the Data Subject means any **freely given**, **specific**, **informed**, and **unambiguous** indication of the Data Subject's wishes by which he/she, by a statement or by a **clear affirmative action**, signifies agreement to the processing of Personal Data relating to him/her.
- True consent is difficult to obtain
  - must be clear, explicit and voluntary (not conditional or in legalese)
  - Neither implied nor negative consent (including, for example, pre-ticked boxes) are sufficient
  - Is there an imbalance of power where a data subject believes consent must be given?
- Consent can be withdrawn.
- May be able to rely on another legal basis.

12

Subsets of Personal Data

- Special Categories of Data (processing generally prohibited):
  - racial or ethnic origin;
  - political opinions;
  - religious or philosophical beliefs;
  - trade union membership;
  - genetics or biometrics;
  - health; and
  - sex life or sexual orientation.
- Exception - consent
- Additional rules apply to children's personal data, and criminal records.

13

Rights of Data Subjects

- Right to transparency/right to be informed.
  - Notice: the 5Ws, individual rights, where to lodge complaints, legal basis for processing, right to withdraw consent (if consent is legal basis).
- Right to access.
- Right to rectification.
- Right to erasure.
- Right to restrict processing.
- Right to object to processing (incl. direct marketing).
- Right to data portability.
- Rights re: automated decision-making or profiling.

14

Data Breach

- Definition of data breach under the GDPR is broad:
  - "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."
- Organization must notify applicable Supervisory Authority within **72 hours** of becoming "aware," UNLESS unlikely to "result in risk to individuals' rights/freedoms."
- Organization must notify affected individuals "without undue delay" where likely to "result in 'high' risk to individuals' rights/freedoms."
- Specific notification requirements

Enforcement and Penalties

- Supervisory Authorities
- High: 4% of annual global turnover [revenue] or €20 Million (whichever is greater).
  - Failure to obtain proper consent
    - See Google's $56.8 million fine
  - Failure to permit Data Subjects to exercise their rights.
    - Including "erasure" and "portability."
  - Transferring data outside the EU without appropriate safeguards.
- Low: 2% of annual global turnover [revenue] or €10 Million (whichever is greater).
  - "Minor Infringements."
  - Failure to maintain adequate records of consent.
  - Failure to make breach notifications.

Enforcement and Penalties

- Individual/group claims for damages permitted.
  - Individuals may:
    - submit complaints to a supervisory authority, and go to court;
    - seek compensation for material and non-material damages (i.e., distress) resulting from a breach of one or more of the stated individual rights; and
    - direct a not-for-profit entity (to be established in each Member State) to lodge a complaint.
  - A not-for-profit entity created in the EEA may also lodge complaints and seek damages on its own accord.

The GDPR and You: Practical Tips

- Conduct an internal audit on the data you collect
  - Analyze who you're collecting data on, how you're collecting it, how you store it, how you share it
- Review and revise your website's privacy policy so that it complies with GDPR requirements. Include individual rights, contact points and procedures.
- Get cyber security insurance. If you already have it, review your coverage to incorporate any policies you implement for GDPR compliance.

18

What Your Company Must Know!

- **Individual Rights Request**
  - Data Subject may make a request verbally or in writing to **ANYONE** at your company! Have a system in place that enable you to swiftly respond.
    - **One calendar month for response to data subject**
- **Breach Notification**
  - If anyone in your company notices a data breach, lose technology or data in any form, he or she should immediately inform a supervisor.
    - Follow all measures possible to secure data.
      - **72 Hours to report to supervisory authority if reporting is found to be necessary.**

19

What Your Company Must Know!

- **Data Collection**
  - Assume any data collection implicates the GDPR.
    - Carefully consider how and why you are collecting information.
- **Data Transfers**
  - Assume any transfer of data implicates GDPR.
    - **vendor contracts
- **Data Minimization**
  - Collect only what you need, have and document a legitimate basis for it, and keep it for only as long as that basis exists

20

Key Takeaways

- **US businesses may be subject to GDPR, depending on operations.**
- **GDPR continues to evolve**:
  - Member States are directed to set their own rules or have authority to deviate and regulatory bodies continue to develop guidelines.
- **Many GDPR obligations are best practices for compliance with US laws.**
  - Good governance and good data hygiene. Data protection "by design and by default." Focus on progress, not perfection.
- **Be more cognizant of data collection, sharing, and transfers!**
- **Review your current practices and policies. Update as necessary.**

21

California Consumer Privacy Act

- Effective Jan. 1, 2020
- Purpose - provide (California resident) consumers greater control over their personal information, promote transparency in businesses' data practices, and safeguard against the misuse of consumer data
- Applies to businesses that collect such personal information and
  - have an annual gross revenue exceeding $25 million;
  - annually buy, receive, sell, or share the personal information of 50,000 or more consumers; or
  - derive 50% or more of its annual revenues from selling consumers' personal information
- Damages
  - $7500 per violation – attorney general enforcement
  - $100-$740 per violation – private right of action

22

New York Senate Bill 224

- Similar to California Consumer Privacy Act
- Introduced January 2019
- All individuals (New York residents) have a right of privacy in information pertaining to them," and businesses (who do business in NY) must provide consumers with transparency about how consumers' personal information has been shared with or sold to third parties

23

Questions?

- Fred J.M. Price
- fjprice@bsk.com

24