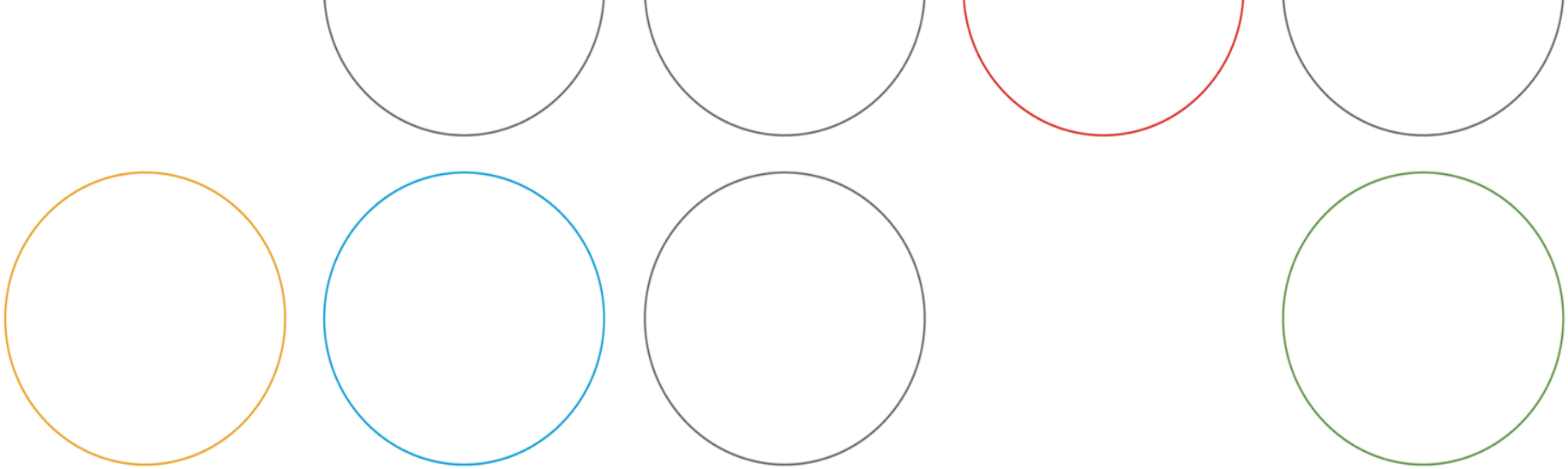


GDPR is Coming
Five Things You Can Do Now To Prepare

WINSTON & STRAWN

Our Presenters

Monique Bhargava

MABhargava@winston.com

Peter Crowther

Pcrowther@winston.com

Sheryl Falk

Sfalk@winston.com

Rob Newman

Rnewman@winston.com

The Basics

- General Data Protection Regulation
  - Effective May 25, 2018
- Replaces the current Directive
- Penalties
  - Up to the greater of €20 million or four percent of the company's worldwide turnover

Five Things You Can Do Now To Prepare

1. Decide if GDPR Applies to You
2. Determine Where Your Data Comes From and Where it Goes
3. Establish Mechanisms to Allow Data Subjects to Exercise Their Rights
4. Update Your Data Breach Response Plans and Privacy Notice
5. Prepare to be Accountable

Decide if GDPR Applies to You

WINSTON & STRAWN

In a Nutshell

- GDPR applies to companies involved in the ***processing*** of ***personal data*** of individuals located in the EU

What is Processing?

- Any operation or set of operations which is performed on personal data or on sets of personal data

What is Personal Data?

- Any information relating to an identified or identifiable natural person

- Conceptually quite broad
  - Online identifiers
  - Cookie information
  - Location Data
  - Device IDs
  - Sensitive personal data

Should a company that has no “on the ground” operations in the EU really care about GDPR?

Controller or Processor?

Controller	• Determines the purposes and means of the processing of personal data
Processor	• Processes personal data on behalf of the controller

What Companies Have to Comply?

1. A controller or processor that maintains an “establishment” in the EU if that EU establishment processes personal data, regardless of whether the processing actually takes place in the EU

2. A controller or processor not established in the EU “where the processing activities are related to offering goods or services to data subjects in the [EU]”

3. A controller or processor not established in the EU if that the entity processing personal data of data subjects in the EU and that processing is related to the “monitoring” of “behavior” of data subjects within the EU

Do You Direct Your Processing Activities to EU Data Subjects?

- What languages do you use?
- What currencies do you accept?
- At whom do you direct your advertising?

Are You Monitoring Behavior of EU Data Subjects?

- Consider online behavioral advertising
- Other Internet profile
- Offline profiling
- Employee monitoring

When is GDPR Not Applicable?

- Activities not covered under EU law;
- Activity of a EU Member State in furtherance of a common foreign or security policy of the EU;
- Activity performed by a natural person in furtherance of a purely personal or household activity;
- Processing by the EU itself; and
- Activity performed by national authorities to prevent, investigate, or prosecute criminal offenses, or in furtherance of a judicial function.

Recap

- **Does GDPR apply to my organization?**
  - GDPR applies where an organization processes information relating to EU residents and answer to any of the following questions is “yes”:
    - The organization has an establishment in the EU;
    - The processing relates to the organization’s offering of goods or services to EU residents; or
    - The processing relates to monitoring or profiling of EU residents

Determine Where Your Data Comes from and Where it Goes

WINSTON & STRAWN

The Value of the Data Map

- You need to get a handle on your data flows since under GDPR, personal formation may be used only for the purpose for which it was collected

- Consider:
  - Whose data do you have?
  - What data elements are included?
  - Where is it stored?
  - Why do you have it and how long will you keep it?
  - What processors and sub-processors are you using?

Do you have a *lawful basis* for processing EU personal data?

Necessary for performance of a contract with the data subject

Necessary for compliance with a legal obligation

Necessary to protect "vital interests"

Necessary for the performance of a task in the public interest

Legitimate interests that aren't overridden by the data subject's interests

Consent

“Legitimate Interest”? Consent?

- Legitimate Interest requires a balancing of the legitimate interests of the controller against the interests and fundamental rights of the data subject.

- Consent requirements:
  - Voluntary, affirmative statement or act
  - Freely given
  - Specific
  - Informed
  - Subject to being withdrawn by data subjects

Do you have a lawful basis for processing EU *SENSITIVE* personal data?

- Racial or ethnic origin
- Political opinions
- Religious affiliation
- Philosophical beliefs
- Union membership
- Health
- Sexual orientation
- Genetic data
- Biometric data

Using a Third Party Processor?

Only give to them for limited/specific purpose

Make sure they give level of protection required

Make sure they use information consistent with your obligations

Require them to notify you if they can't live up to their requirements

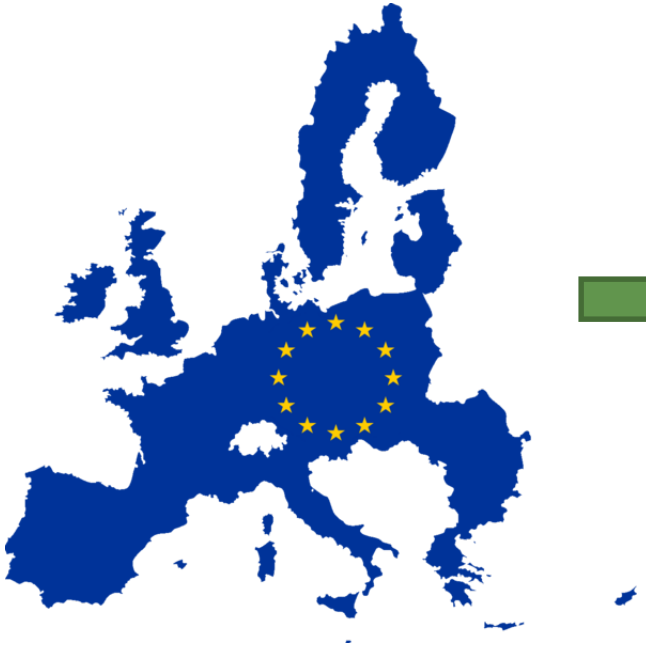
Have a contract in place that says:

- You act only on our instructions
- You give appropriate safeguards
- You will help us respond to people who exercise rights

If they notify you they can't live up to their obligations, then:

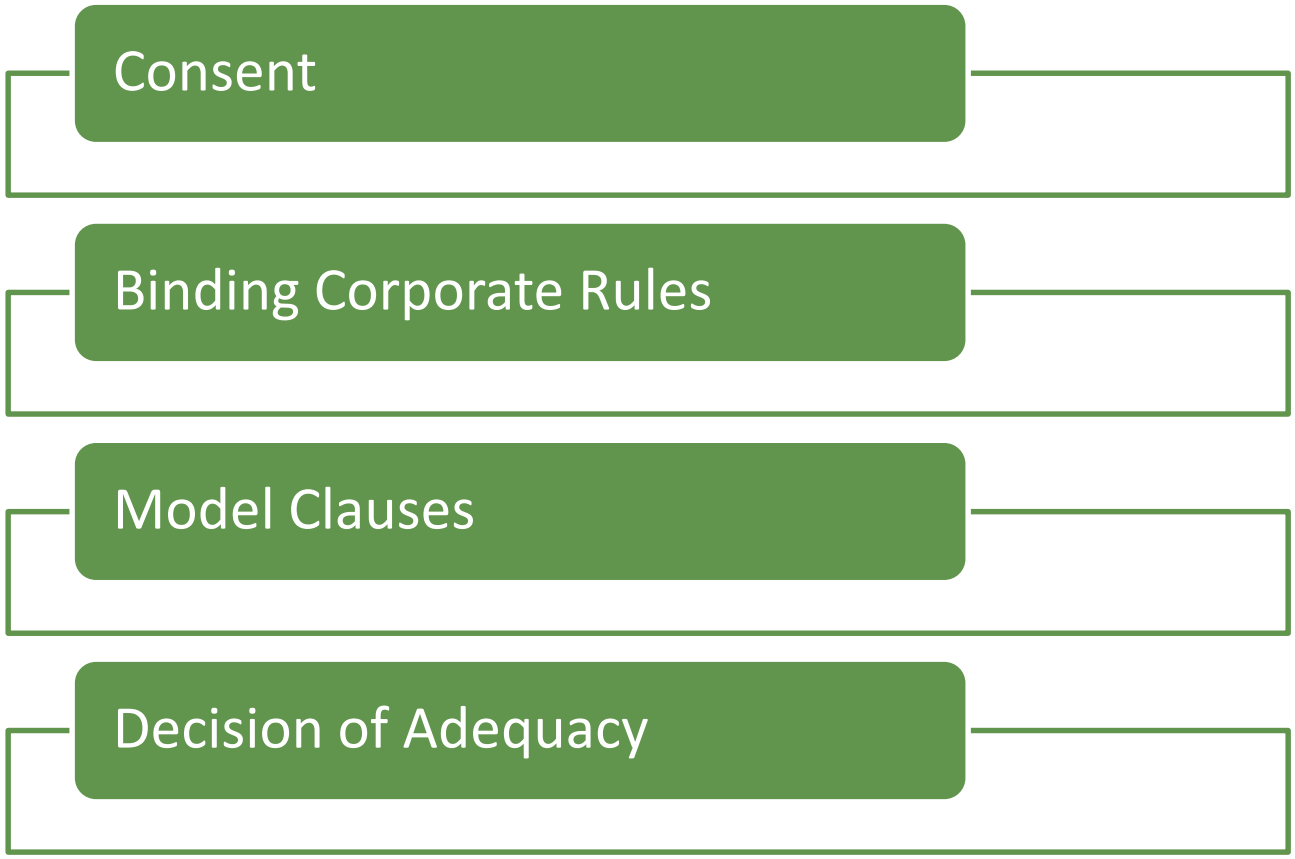
- Stop them from further processing

Transferring Data from the EU to the US?



Data transfers

EU Data Transfer Restrictions, Unless:



Decision of Adequacy

Entire Country

- Andorra
- Argentina
- Canada
- Faeroe Islands
- Guernsey
- Israel
- Isle of Man
- Jersey
- New Zealand
- Switzerland
- Uruguay

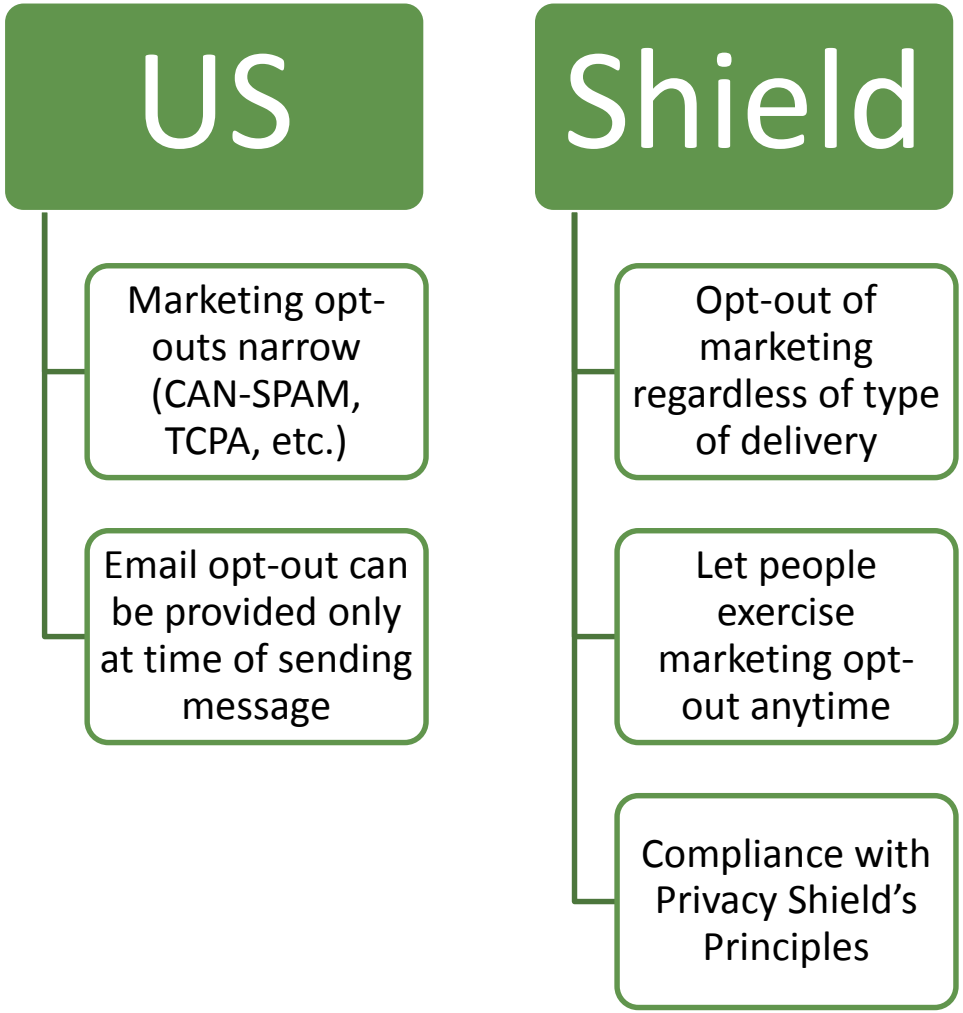
Safe Harbor

- For US companies
- ECJ decision ruled no longer adequate Oct. 2015
- Renewals will stop Oct. 31, 2016

Privacy Shield

- Replaces Safe Harbor
- Started accepting applications Aug. 1, 2016

How Does Privacy Shield Differ From US Law?



Privacy Shield vs. Model Clauses

	Model Clauses	Privacy Shield
Internal training and review requirements		✓
DoC and FTC scrutiny and clear enforcement procedure		✓
Mandatory arbitration		✓
Modeled off of EU Directive	✓	✓
Specific to data set described as being transferred	✓	✓
Registration required with some DPAs	✓	
Can tailor easily to one data transfer set	✓	

Privacy Shield vs. Consent

	Consent	Privacy Shield
Works only if have direct relationship with individual	✓	
Criticized by some DPAs as inadequate, especially in HR context	✓	
Requires specific language when communicating data practices	✓	✓

Privacy Shield vs. BCRs

	BCRs	Privacy Shield
Applies only to intra-company transfers	✓	
Must be approved by DPA	✓	
Application process can take several years	✓	
Would need supporting procedures to implement and effectuate	✓	✓
Core principles adhere to the EU Data Privacy Directive	✓	✓
Application to a US regulatory body		✓

There are Principles; What Do They Really *Mean*?

Automatic Processing and Profiling

- GDPR limits the use of “automatic processing”—or data processing done without any “human intervention
  - Individuals have the “right” not to be the subject to decisions based solely on automated processing, including profiling
- “Profiling” consists of any automated processing of personal data used to evaluate a data subject’s personal characteristics (e.g., health, interests, work performance)
  - Controllers are required to inform a data subject of the use of profiling techniques—regardless of whether the profiling is done through automated or manual processing

Establish Mechanisms to Allow Data Subjects To Exercise Their Rights

WINSTON & STRAWN

Consent and Withdrawal of Consent

- To constitute consent, an affirmative action or step must be taken (e.g., checking a box, written signature, etc.)
  - GDPR drafters specifically indicated that “silence, pre-ticked [pre-checked] boxes, or inactivity should not…constitute consent.”
  - Requests for consent should also not be buried within other language

- Companies will have difficulty providing that consent was valid if there is a power discrepancy between the individual and the organization

- After obtaining valid consent, individuals may still withdraw their consent at any time, and by a method that is at least as convenient as it was to give consent

Keeping Track of Consent

Activity	Method of Consent	Post-Consent Opt-Out
Signing up for email newsletters	Online, un-checked, check box that describes how information will be used and explains right to opt out and how	Using the mechanism that was initially described, like having a mechanism in the message being sent that lets a person "click" to opt out or letting people email optout@company.com to opt out
Credit checks for new customers	Clear consent document, separate and apart from other agreements that clearly discloses the purpose of the credit check, the information that will be collected, how it will be used, and any third-party vendors that may receive the information.	In the consent agreement, provide opt-out instructions and a point of contact for any questions relating to opt outs (likely the DPO).
Payment processing	Obtain consent when initially opening the account via a specific consent-agreement to collect and process payment information.	In each purchase order provide opt-out instructions and a point of contact for any questions relating to opt outs (likely the DPO).

Give People Access to Information

- Upon request, companies must provide individuals with:
  - A confirmation regarding whether the company is processing personal information relating to them. If yes, then must inform:
    - Why
    - What categories
    - Length of storage
    - Sources of data
    - Sharing
    - Automated processing
  - A copy of the personal information
  - The ability to complain to the DPA
  - The ability to correct, amend, or delete

The Right to Be Forgotten

- Requires data controllers to erase a data subject's personal information upon request in the following circumstances:
  - the data is no longer necessary for the original purposes of collection
  - the data subject has withdrawn consent for the processing
  - the data subject objects to data processing and there are no "overriding legitimate grounds" for the data processing
  - the data was unlawfully processed
  - an EU Member State's law requires erasure of the information, or
  - the data subject is a child

The Right to Rectify and Restrict

- GDPR mimics the Privacy Directive in ensuring that data subjects can obtain corrections of incomplete or inaccurate personal data from the controller.

- The controller must make such corrections “without undue delay.”

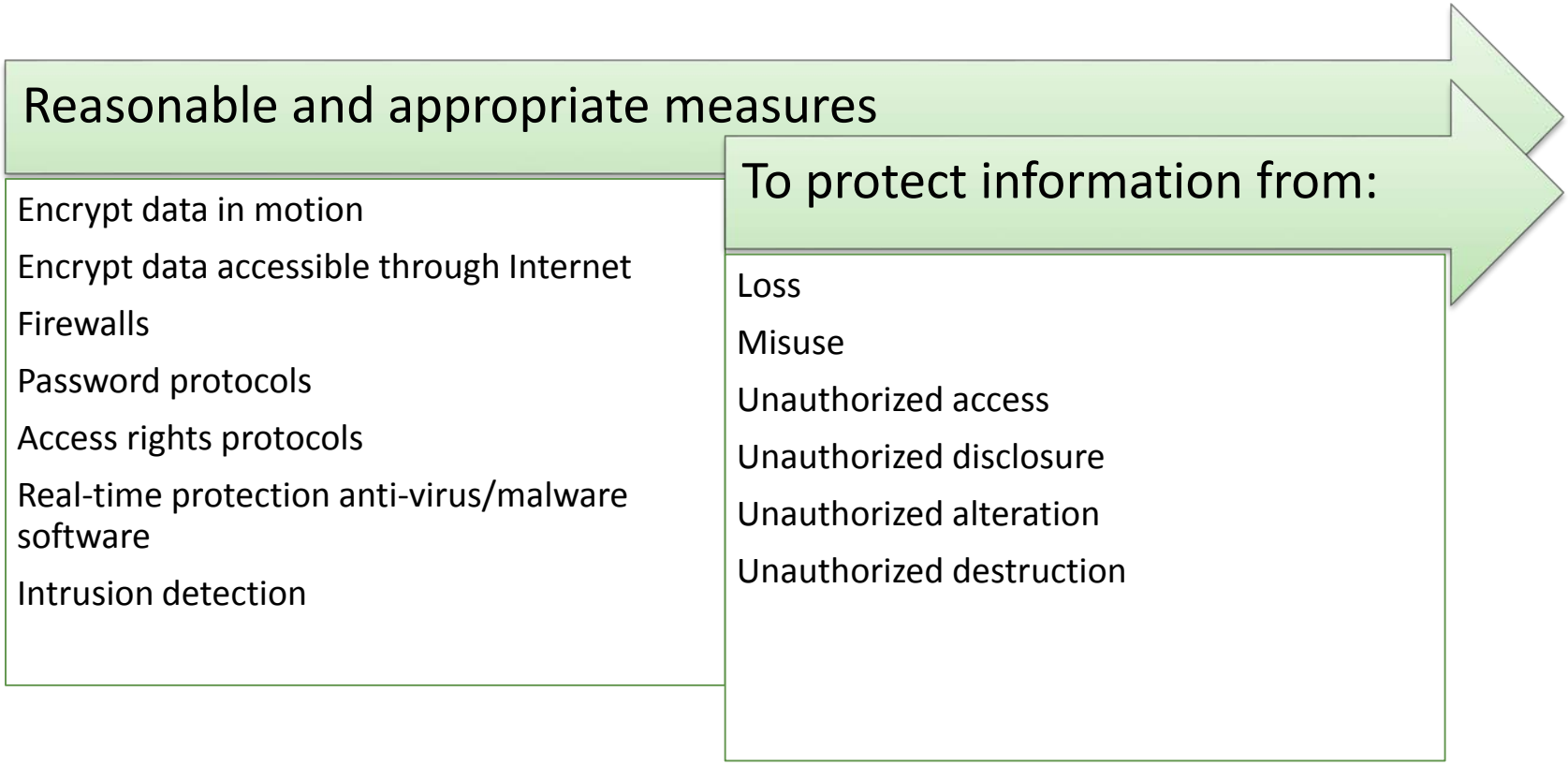
Data Portability

- Companies must give personal data about the requestor that the company maintains in a “commonly used and machine-readable format”

- According to guidance issued by WP29, individuals do not have the right to request data that they themselves did not provide to a company

  - In other words, inferred or derived data (e.g., a credit score calculated by a company based on information provided by the person) falls outside the scope of the right to data portability

Security



CLE Presentation Code

15439

Update Your Data Breach Response Plans and Privacy Notices

WINSTON & STRAWN

Breach Obligations

- Data controllers and Processors are subjection to personal data breach notification obligations
- Broader breach trigger than US notification laws
- Notification within *72 hours* (!)
- Non-compliance can lead to significant administrative fines - 10 million Euros or 2% of total worldwide annual turnover

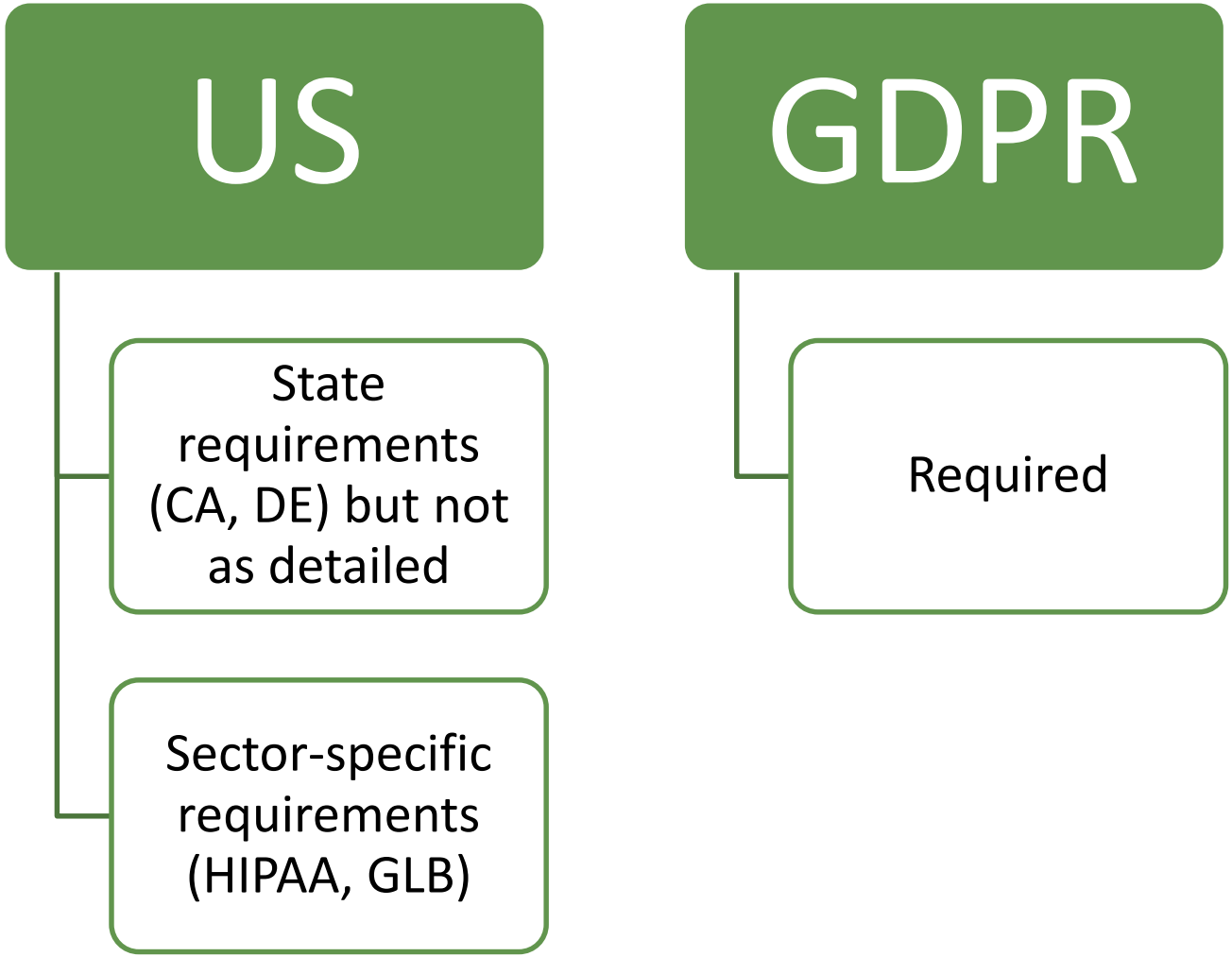
Exceptions to Breach Obligations

- No reporting if:
  - The breach is unlikely to result in a high risk to the rights and freedoms of data subjects;
  - Appropriate technical and organisational protection were in place at the time of the incident (e.g. encrypted data); or
  - This would trigger disproportionate efforts

Update Your Privacy Notices

1. What personal information you collect (including sources of data)
2. Purposes for collecting
3. With whom you share and why
4. Cross-border data transfers
5. Contact info
6. Access/correction/erasure rights
7. Rights regarding choice and consent withdrawal
8. Right to complain
9. Etc.

How Does This Differ From US Law?



Prepare to be Accountable

WINSTON & STRAWN

Determine the Lead EU Country

- Whichever EU country is host to the most significant decisions about the company's data processing will be the company's "main establishment," and that country's DPA will be your principal regulator.

- Brexit complication?

  - The UK ICO has stated that it is in the processing of working with the UK government to provide advice regarding the application of GDPR both before and after Brexit.

Retention and Storage Considerations

Use consistent with notice	Keep only as long as you need for purposes for which provided	Destroy after you don't need (or return)
Make sure information is reliable	Modify/delete if told by person of an error	Update if get a "returned to sender"

Data Protection Officer Required?

Local law

Regular monitoring of data subjects

Sensitive data on large scale

If No DPO, Designated Representatives?

- GDPR requires those with no physical EU presence establish a "representative" in the EU

Privacy Impact Assessment?

- Processing likely to result in high risk to individuals?
- WP29 guidance provides factors controllers should consider in evaluating whether a PIA is necessary:
  - an action that meets less than two of these factors would not require a PIA:
    - **Evaluation or scoring**. For example, grading employees or screening credit applicants.
    - **Automated decision making with significant effect on a person**. For example, the automated refusal of credit.
    - **Systematic monitoring**
    - **Processing Sensitive Personal Data**
    - **Large-scale processing**
    - **Combining or matching separate datasets**
    - **Processing affecting vulnerable individuals**. **Processing using untested technology**.
    - **Bootstrapping**

CLE Presentation Code

15439

Conclusions

Does it Apply?

Where is your data?

Establish Compliance Mechanisms

Update Policies

Be Accountable

Thank You

Monique Bhargava

MABhargava@winston.com

Peter Crowther

Pcrowther@winston.com

Sheryl Falk

Sfalk@winston.com

Rob Newman

Rnewman@winston.com