

# Global Data Privacy & Compliance

June 14, 2018



# Presenters



**Pamela Webb**

**Senior Director, Global Strategy**



**Michele Honomichl**

**Founder, Executive Chairman and  
Chief Strategy Officer**



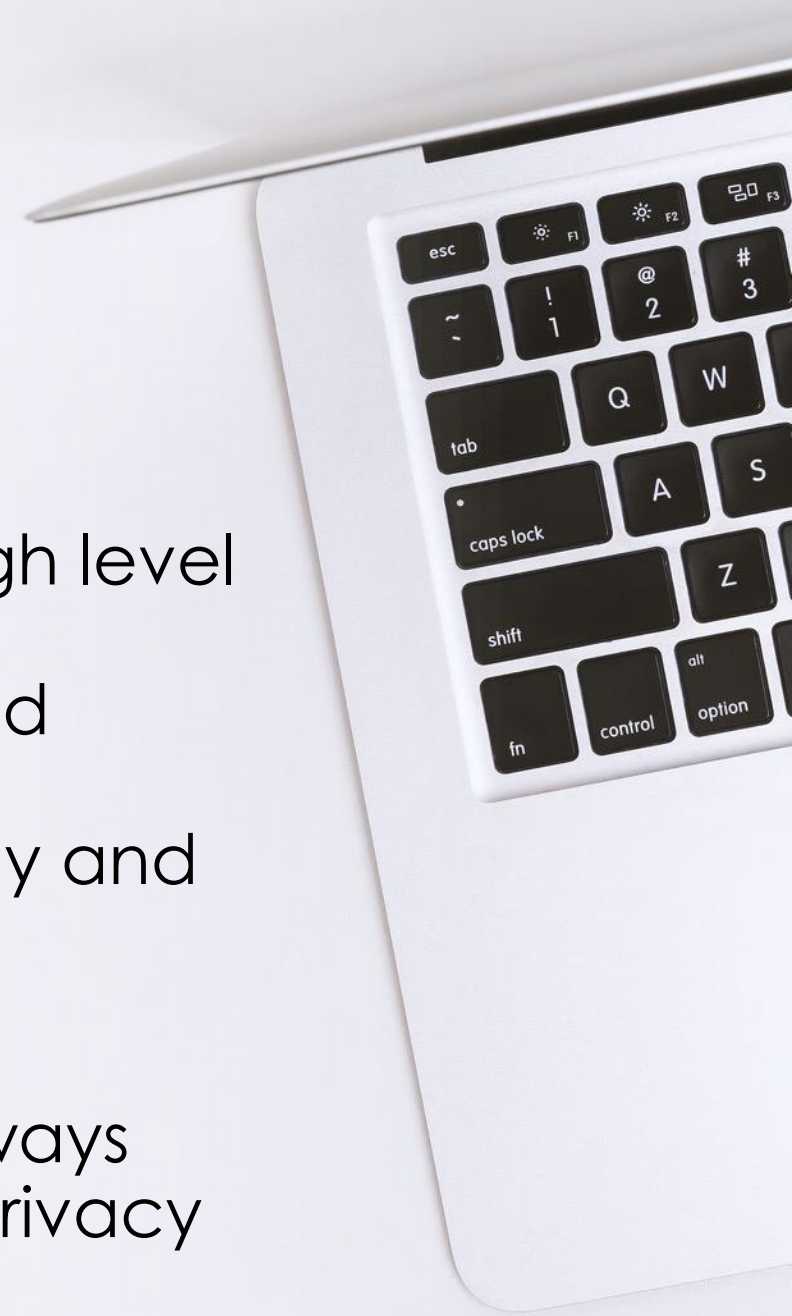


# Privacy is Tough!

## The Fine Print

The purpose of this presentation is to provide a high level introduction to Global Data Privacy & Protection, specifically GDPR, and to share considerations and mutual experiences in global data privacy and protection practices for educational purposes only and does not constitute legal advice.

Due to the sensitive nature and corporate risk, always obtain legal advice before deploying any data privacy and protection initiative for your organization.





# What We're Going to Cover

- Approaches in Data Privacy & Personal Data
- GDPR – What is it & why it matters for U.S. Employers
- Understanding Different Data Roles & Obligations
- How the GDPR protects information & individual rights
- What U.S. Employers should do
- Ongoing Demonstration of Compliance and Protection
- Other Global Trends

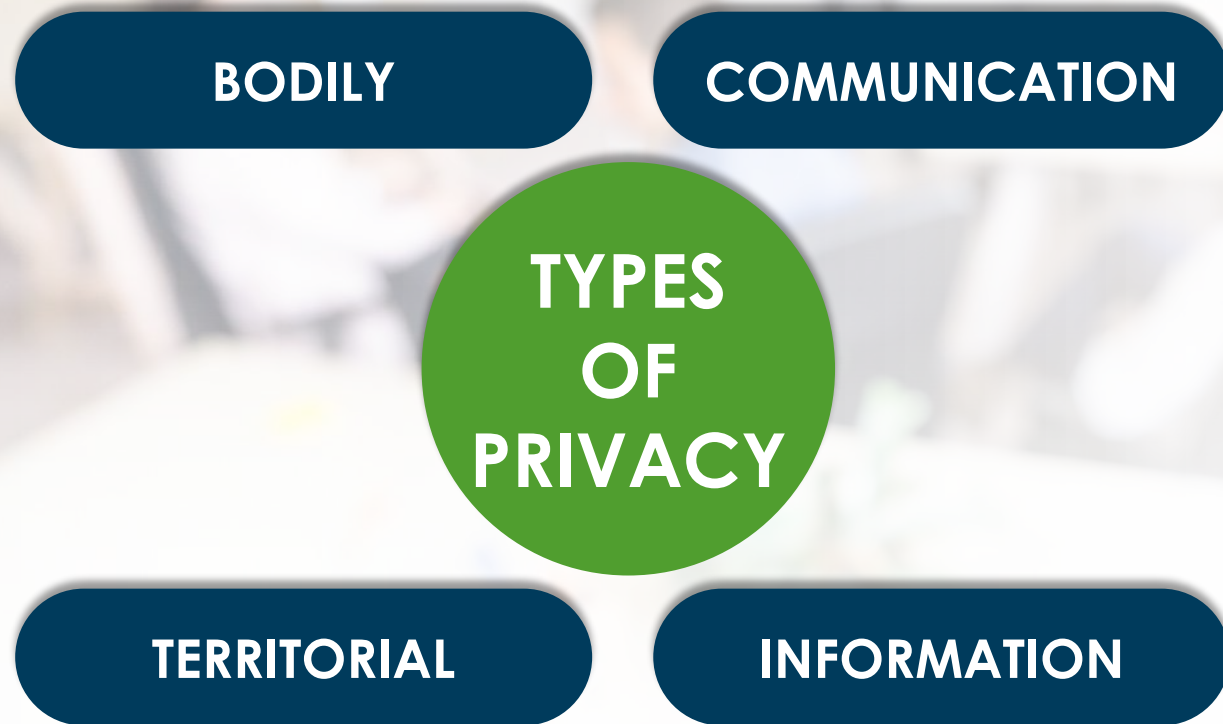


# What is Privacy?

- Defined in 1890 by Harvard Law Review as the “**right to be left alone**”
- The right of an individual to be protected against intrusion into his/her personal life (U.K. 1997)
- Today, Privacy is more described as “**appropriate use.**”



# What information is Private?



**It depends on the ...**

- Specific law or country
- Sector (health, banking)
- Context
  - Home address in the phone book is **Public**
  - Home address provided to a service provider is **Private**



# Personal *versus* Sensitive Personal Data

## PERSONAL DATA

**Information that relates to an identified or identifiable living individual**

- First and last name
- Physical address
- email address
- Telephone number
- Social security number

## SENSITIVE PERSONAL DATA

**Information that can create a bias (conscious or unconscious)**

- Racial or ethnic origin
- Sexual orientation
- Health or medical records
- Religious or philosophical beliefs
- Political opinions
- Criminal records

# Why Should We Care?

Risks of not having adequate privacy and data handling requirements include:

- Legal Compliance
- Reputation
- Investment
- Competition

Ponemon Institute estimates an average breach cost of \$3.5 million in 2017, with a 27% probability that a U.S. company will experience a breach in the next 24 months that costs them between \$1.1M and \$3.8M.

BUSINESS TECH FACEBOOK

## Facebook stock tanks after data breach report, shaving billions off company's market value

By Shannon Liao | @Shannon\_Liao | Mar 19, 2018, 2:58pm EDT

United Kingdom, USA | January 22 2018



The United Kingdom High Court recently issued a landmark liability judgment against the supermarket, Morrisons, following a data breach caused by a rogue employee (*Various Claimants v. WM Morrisons*)



So let's discuss  
how this thing  
called **GDPR**  
came about



# Fundamental Principles

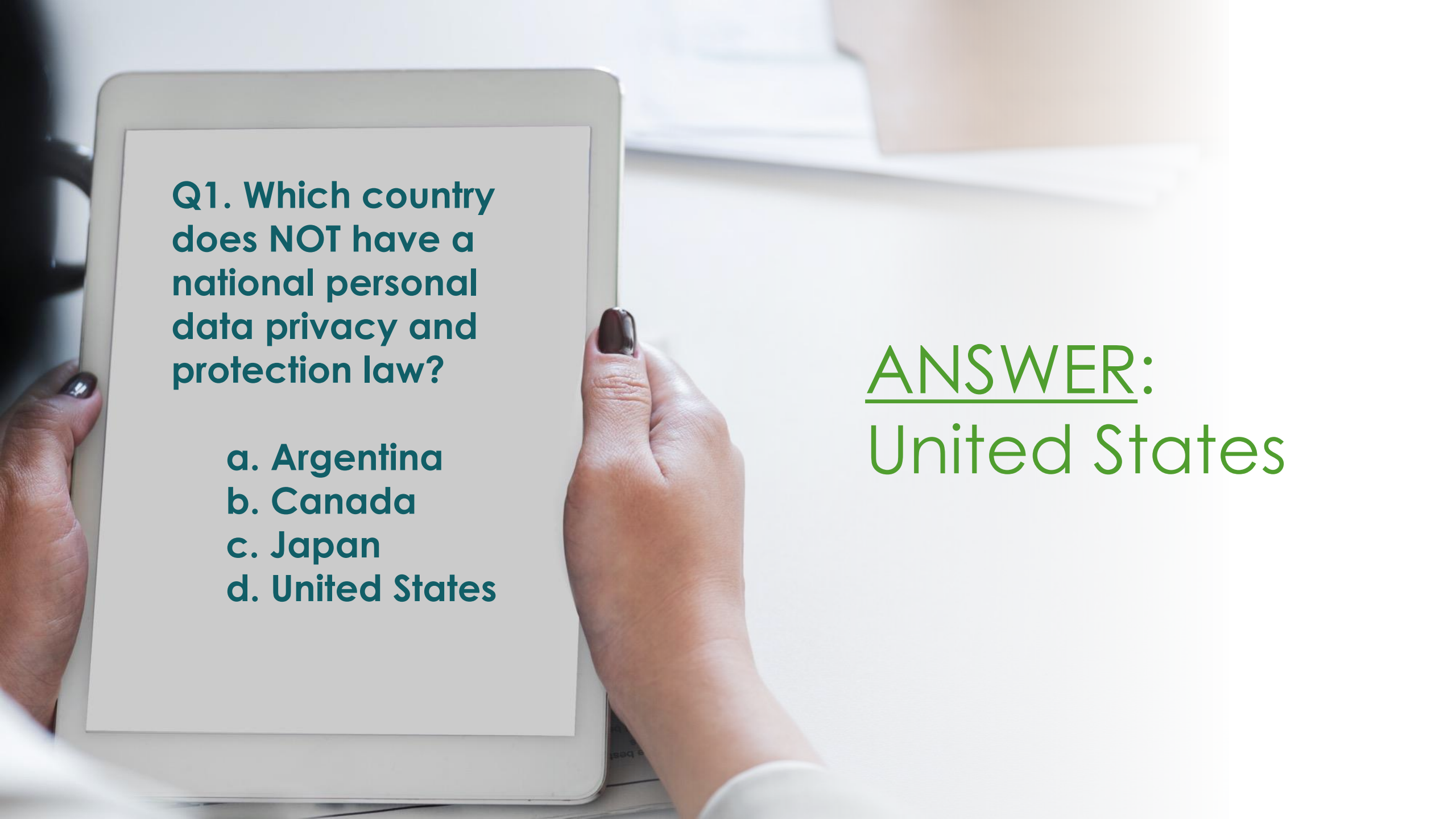
**Organization for Economic Co-operation and Development (OECD) defines fundamental principles for "appropriate use" to include:**

- Collection Limitation
- Data Quality
- Purpose Specification
- Use Limitation
- Security Safeguards
- Openness
- Individual Participation
- Accountability

Followed by the EU Data Directive in 1995 and APEC Privacy Framework





A person's hands are visible holding a white tablet. The tablet screen shows a quiz question in dark teal text. The background is a bright, out-of-focus indoor setting with a desk and some papers.

**Q1. Which country  
does NOT have a  
national personal  
data privacy and  
protection law?**

- a. Argentina**
- b. Canada**
- c. Japan**
- d. United States**

**ANSWER:**  
**United States**

# Varying Privacy Approaches

## EUROPEAN UNION

**Privacy is a basic human right**

**No processing permitted (Opt-in)**

**Comprehensive law**

**Co-regulatory**

## UNITED STATES

**Privacy is a consumer protection issue**

**Processing permitted (Opt-out)**

**Sectoral Law (e.g., HIPPA, GLB)**

**Self-regulatory**

\* EU's areas of concern with the U.S.: Adequacy (of protection and enforcement).



# European Union Directive 95/46/EC

Integral to EU's privacy and human rights law

General principles regulating processing of personal data within the EU



Obligation is within each member country to enact legislation



**Q2. What does GDPR stand for?**

- a. General Data Protection Regulation
- b. Global Data Protection Regulation
- c. General Data Protection Representation
- d. Global Data Protection Representation

ANSWER:  
General Data  
Protection  
Regulation





# The EU Response: General Data Protection Regulation

## WHY:

- The Data Directive was not “law”
- Provide the individual more control
- Need for harmonization and consistency
  - Member State Rules
  - Data Protection Authorities
  - Administration
- Risk-based approach
- Accountability

## WHEN:

Adopted in 2016 but enforceable  
effective May 25, 2018

A person's hands are visible holding a white tablet. The tablet screen shows a quiz question in dark teal text. The background is a blurred office setting with a desk and a laptop.

**Q3. Who is protected under GDPR?**

- a. Individuals with legal citizenship in the European Union**
- b. Individuals residing in the European Union**
- c. Any individual processed in the European Union**
- d. All of the above**
- e. None of the above**

**ANSWER:**  
**All of the above**



# Who is GDPR Protecting?



General  
Data  
Protection  
Regulation

- Applies to all EU countries, even post-Brexit U.K.
- Protects and empowers all EU citizens data
- Processing data for “whatever” the nationality or residence of natural persons
- Article 3(2): *"This Regulation applies to the **processing of personal data of data subjects** who are in the Union "*
- Article 3(1): *"... processing of personal data... **regardless whether the processing takes place in the Union or not.**"*

# New for GDPR

Personal Data  
Definition  
Expanded

Provisions for  
Technology  
(e.g. AI)

Individual  
Rights  
Consent  
Portability  
Erasure

Controller  
AND Processor  
Obligations

Data  
Protection  
Officer

Privacy by  
Design

Breach  
Notifications

Enforcement  
Financial  
Penalties

Enforcement  
Criminal  
Sanctions

**Q4. Which of the following is NOT a basic tenet of GDPR ?**

- a. Purpose Limitation Principle**
- b. Storage Limitation Principle**
- c. Data Minimization Principle**
- d. Data Transfer Limitation Principle**

**ANSWER:**  
**Data Transfer  
Limitation  
Principle**



# GDPR Key Components

1995 EU Directive vs. 2016 GDPR

## EU Data Privacy Directive

Notice

Purpose

Consent

Security

Disclosure

Access

Accountability

## EU General Data Protection Regulation (GDPR)

Lawfulness, fairness, and transparency principle

Purpose limitation principle

Data minimization principle

Accuracy principle

Storage limitation principle

Integrity and confidentiality principle

Accountability principle

# General Data Protection Regulation (GDPR)

## Improvements with GDPR

Many core concepts the same

Greater harmonization of requirements

Risk based compliance approach

## New Challenges of GDPR

Increase enforcement powers

Expanded territorial scope

Consent harder to obtain

Data protection by design and default  
including accountability and governance

Data Protection Compliance Programs &  
Data Protection Officers (DPO)

New obligations of processors

Right to access, rectify, erasure, restriction, data portability,  
object, not be subjected to automated decision making

Strict data breach notification rules

Right to claim compensation

**Q5. What is penalty for Consent infringement?**

- a. Up to €1 million, or 2% country's annual revenue
- b. Up to €10 million, or 2% of country's annual revenue
- c. Up to €5 million, or 4% worldwide annual revenue
- d. Up to €20 million, or 4% worldwide prior annual revenue

**ANSWER:**

Up to €20 million,  
or 4% of the  
**worldwide** prior  
annual revenue



# Why Should a U.S. Employer Care about GDPR?

**U.S. Multinationals with EU residents (or considering entering the EU) are subject to the law**

- **Within the borders of the EU, including employees, independent contractors**
- **Any personal EU data that transfers outside the EU (e.g., global payroll reporting and analytics)**
- **Including Cloud based service providers and subcontractors**

**...and the BIG reason? Fines of up to 20 MILLION EURO or 4% of annual worldwide turnover**

# GDPR's Expanded Definition for Personal & Sensitive Data

## PERSONAL DATA

Information that relates to an identified or identifiable living individual

- First and last name
- Physical address
- email address
- Telephone number
- Social security number
- **Location Data**
- **Online identifiers (IP, cookies)**

## *SENSITIVE* PERSONAL DATA

Information that can create a bias (conscious or unconscious)

- Racial or ethnic origin
- Sexual orientation
- Health or medical records
- Religious or philosophical beliefs
- Political opinions
- Criminal records
- **Genetic data**
- **Biometric data**



# This is HR & Payroll's Data

- Personnel files
- Onboarding
- I-9s
- Leave
- Timecards
- Timecard corrections
- Paystubs
- W-2s
- W-4s
- Discipline
- Performance reviews
- Doctor's notes
- Supervisor notes
- Direct deposit information
- Handbook acknowledgements
- Resumes
- Training paperwork
- Certifications
- Work comp
- Injury reports
- Employment contracts
- EEO-1s
- Affirmative Action Reports
- & more!





# Reframing Idea

- The data no longer belongs to HR & Payroll
- Data belongs to the employee
- HR & Payroll only has consent to use it for legitimate purposes
- Privacy by design & default as legal requirements

# How Does the GDPR Work?

- Many provisions applicable to HR & Payroll
- Whenever an organization gathers or processes information from an individual (who resides in the EU), consent must be  
“freely given, specific, informed and unambiguous” and  
“...by a statement or by clear affirmative action”
- An individual has the ability to withdraw his/her consent at any time
- HR & Payroll needs to maintain quality information (accurate, up-to-date)





# Freely Given Consent

- Because of the power imbalance between employer & employee, consent is not generally considered freely given
- As a requirement for a position, probably not freely given
- Not a condition of employment (probably)
- Separate
- Meaningful
- Clear & plain language
- “Genuine choice & control”



# How to Get Consent

- Not an easy click-thru
- Clear language that explains the individual's rights to her own data
- Separate pop-up
- Separate document



# Transparency

A background image showing a group of people in business attire sitting around a wooden table. One person is holding a tablet, and another is pointing at the screen. The image is partially obscured by a dark overlay on the left side where the text is located.

- Explaining to individuals how you'll use data
- May mean a policy
  - Explains who has access
  - How you process data
- Specificity
  - “We may use your data to improve services” will likely not pass muster
  - “We may use your data to make employment decisions”



# Right to Portability

## For Employees

- As Data Owner, I have the right to take my personal data with me

## Preparedness

- Define data scope
- Map systems and data flow
- Define delivery mechanism





# Right to Erasure (to be Forgotten)

## For Employees

- As the Data Owner, I have the right to have my data removed

## Preparedness

- Define data scope
- Map systems & data flow
- Define policy for deletion, anonymization or pseudonymization



# Before You Erase...

## General Business

- Do record retention laws still apply in EU or U.S.?
- Is any litigation hold in effect?

## Employee Impact

- Is the individual terminated?
- Is identification needed for post-termination benefits/pension coverage?



# The Other Rights



**Right to  
access data**



**Right to  
rectification**



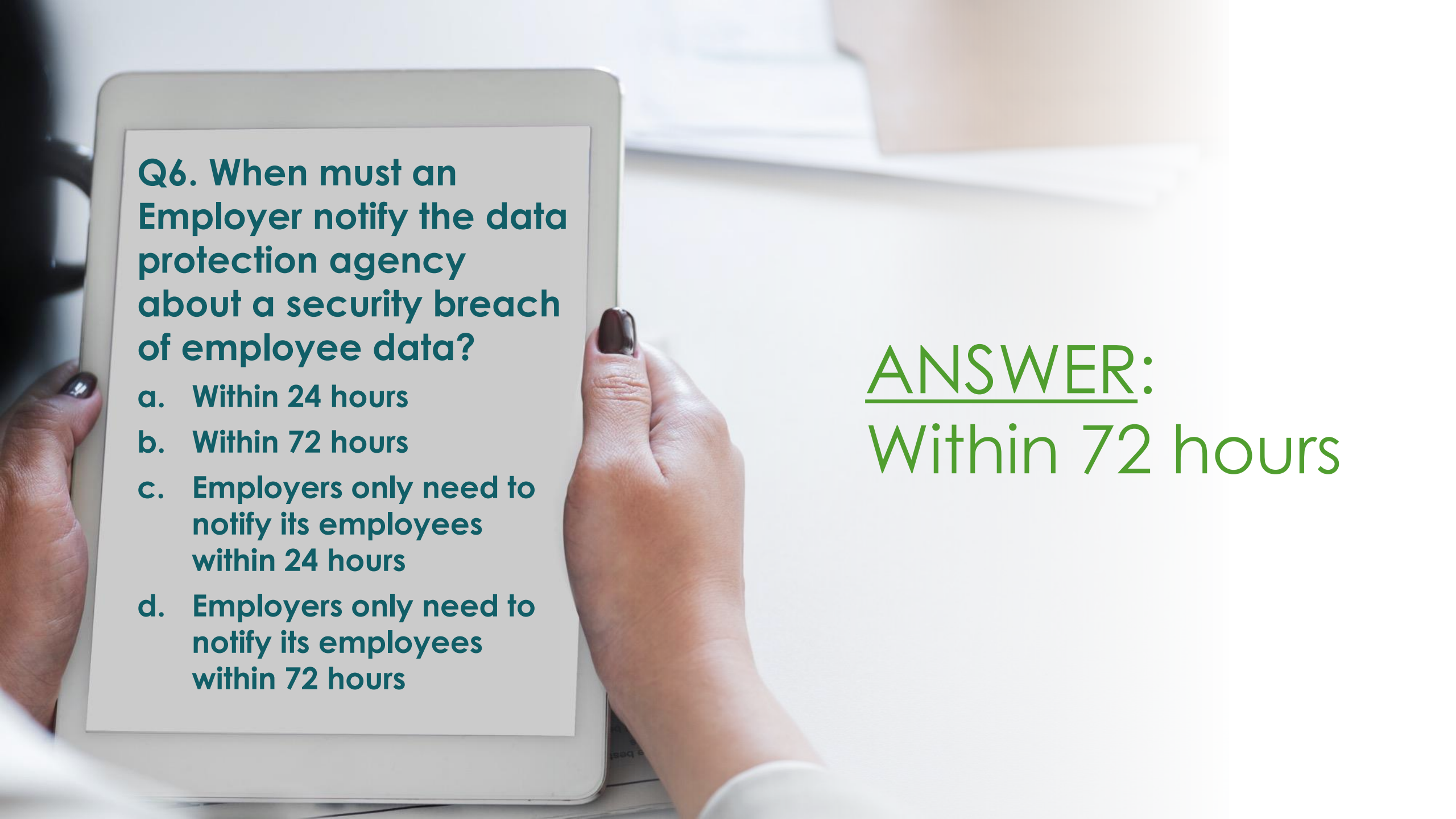
**Right to restrict  
processing**



# What About AI?

A woman with long dark hair, wearing a dark blazer, is shown from the chest up, looking off to the side with a thoughtful expression. In the background, there is a glowing blue network diagram that resembles a brain, composed of interconnected nodes and lines, with some nodes emitting bright light.

- Pseudonymization
- Anonymization
- If we don't know who this data belongs to, theoretically, we can use it
- HUGE role in use of AI
- Care with how re-identifiable information truly is

A person's hands are visible holding a white tablet. The tablet screen shows a quiz question in a dark teal font. The background is a blurred office setting with a desk and some papers.

**Q6. When must an Employer notify the data protection agency about a security breach of employee data?**

- a. Within 24 hours**
- b. Within 72 hours**
- c. Employers only need to notify its employees within 24 hours**
- d. Employers only need to notify its employees within 72 hours**

**ANSWER:**  
**Within 72 hours**



# What If There's a Breach?

- Employers who suffer a breach of employee data must notify the data protection agency where the employee resides within 72 hours
- Applies only to EU residents
- Requires knowing & monitoring for breaches





A close-up, high-angle shot of a red running track. The track is marked with white lines forming lanes. Large white numbers 1, 2, 3, and 4 are painted on the track, indicating the lane numbers. The text "Steps to Compliance" is overlaid in white, bold, sans-serif font, centered on the track.

# Steps to Compliance





**1**

**Legal/  
Privacy**

**Security**

**Marketing**

**HR**

**Identify  
Your Team**



# Do I need a Data Privacy Officer (DPO)?

Article 37(1) GDPR requires data controllers and processors to designate a DPO if they **process large-scale amounts** of sensitive data on a regular and systematic basis

- Reports to the top executive
- May be an employee or externally appointed
- Statutorily independent and protected
- Responsibility is to the **data not the company**



2

# Identify Personal Data Reach



# What Should You Do?

## Figure out where all your employee data is

- Conduct an audit
- Review with vendors & IT team

## Work with your vendors

- Identify them all
- Ask about their GDPR efforts
- Modify contract language where necessary
- Ask about how they use data



3

Document,  
Document,  
Document

Identify Basis:  
Processing Data

Policies & Procedures

Conduct DPIAs

Appoint DPO?



# What Should You Do?

## Define your policies & processes

- Data breach notification policy
- Overall scope & approach to respond to individual requests
- Handbook or department policy revisions

## Notify employees of the GDPR

- How you keep data
- How you use data
- How others may be using their data



4

# Requests from Individuals

Right to Restriction

Right to Rectification

Right to Erasure

Right to Transparent Info.

Right of Access/Data Portability

Objection to Automated Decision Making

5

**Confirm  
Identity**





A top-down view of a workspace on a dark wooden desk. On the left, a silver laptop is open, displaying a web application with a sidebar and a main content area. Next to it is a small white mug with a green handle, filled with dark coffee. To the left of the laptop is a yellow notepad with a black pen resting on it.

# GDPR Takeaways

- While not all U.S. employers are subject to the GDPR provisions, it provides a “best practices” framework that can apply to all people data
- Consider how you obtain consent
- Review data security & data protection protocols
- Hold vendors accountable





# GDPR Key Compliance Components

## GDPR Key Compliance Components



**Privacy  
Shield**



**Data  
Protection  
Agreement**



**Standard  
Contractual  
Clauses**



**Data  
Importers,  
Exporters,  
Controllers &  
Processors**



# What Are the Main Buzz Words of GDPR?

- Data Subject
- Data Controller
- Data Exporter
- Data Processor
- Data Importer
- Privacy Shield
- Data Protection Authority (DPA)
- Data Processing Addendum (DPA)
- Binding Corporate Rules
- Standard Contractual Clauses
- Model Clause

# Privacy Shield Framework

## What Is It?

Replacement of  
Safe Harbor with  
stronger controls

## Basic Tenets

- Company Obligations
- Enforcement
- Government Access
- Monitoring





**Q7. Which of the following is NOT true about Privacy Shield?**

- a. It is based on similar tenets as Safe Harbor
- b. It requires prompt reply to complaints
- c. Its policy is reviewed every two years by U.S. and Europe
- d. Companies can self-certify

ANSWER:  
Its policy is reviewed every two years by U.S. and Europe

# How Does It Differ from Safe Harbor?

- Tighter corporate regulations
- Redress is with the company, plus arbitration mechanisms
- Limitations on government access to private information
- Review of policy annually







# Privacy Shield – A New Policy for the USA & Europe

## Requirements for Companies Transferring Data:

- Self-certify annually that they meet the requirements
- Display privacy policy on their website
- Reply promptly to any complaints
- Cooperate and comply with European Data Protection Authorities



# How Does It Come Together?

**Employees**



**Data Subject**

**Company**



**Data Controller &  
Data Exporter**

**Payroll Processor**



**Data Processor &  
Data Importer**



# Adequate Safeguards

A laptop is shown from a slightly elevated front angle, resting on a dark, textured surface. The screen displays a bright, multi-colored light effect that transitions from purple on the left to red in the center and blue on the right. This light effect also appears to emanate from the keyboard area, creating a rainbow-like glow across the keys. The background is dark and out of focus.

**Binding  
Corporate  
Rules**

**Standard  
Contractual  
Clauses**

**Code of  
Conduct**

**Certification**

# Binding Corporate Rules (BCRs)

**BCRs are internal rules for data transfers within multinational organizations.**

- **Organizational specific** code of conduct
- Select lead Data Processing Authority (DPA)
- Relevant DPAs review and comment
- Final agreement allows organization to transfer to non-adequate countries within the organization

## Challenges

- The process is time-consuming (12-18 months)
- Can be costly for an organization with multiple countries
- Exposes the organization to ambiguous regulatory oversight



# Compliance Packages

## Components of a GDPR Contract Addendum Package:

- **Data Processing Addendum (DPA)**
- **Standard Contractual Clauses (SCC)**
  - **Appendix 1: Locations Covered**
  - **Appendix 2: Data To Be Exported**
  - **Appendix 3: (Data Transfer Agreement)**





# Compliance Packages

**Data Processing Addendum (DPA):** Defines What Data and How the Data is Managed Between the Data Controller and Data Processor

## Data Controller:

**Entity that determines the means of the data processing**

- Being in compliance and demonstrating compliance
- Accountability of the Principles of GDPR (Integrity, purpose limitation, storage limitation, accuracy, data minimization, and lawfulness)
- Data protection by design and default
- Recordkeeping of processing activities

## Data Processor:

**Entity that processes data on behalf of the controller**

- Provide transparency of sub processors to controllers
- Demonstrate compliance and security
- Cooperate with Supervisory Authorities
- Contract with Data Controller
- Recordkeeping of processing activities



**Q8. Which is NOT true about standard contractual clauses?**

- a. Outlines the responsibilities between the data exporter and data importer
- b. Can be negotiated between the exporter and the importer
- c. Outlines the data to be transferred between the two parties
- d. Details the security controls of the data importers

**ANSWER:**

Can be **negotiated** between the exporter and the importer

# GDPR Key Components

## Standard Contractual Clauses

### What are they?

A model contract for the transfer of personal data from a data exporting organization to a data importing organization to a third country

### Information Needed by Orgs That Are Party to the SCCs:

- Identifying information for both organizations
- Determining categories of data being transferred the categories of data subjects whose data will be transferred

### Data Exporter

- A description of the purpose(s) of the transfer
- An explanation of the recipients whom the transferred data may be disclosed

### Data Importer

- Information regarding the processing operations to be performed
- A description of the technical & organizational security measures the Processor has implemented to protect the data



# Compliance Packages

## Standard Contractual Clause (SCC) Outline Responsibilities

### Data Exporter

- In compliance with data protection law
- Instruct the data importer to process the data on its behalf
- Ensure data security at all levels
- Ensures the data subject has given consent
- Forward any notification to the data protection supervisory authority

### Data Importer

- Only process personal data to provide services
- Implement technical security for data
- Promptly notify Controller of any security breach incident
- Ensure compliance of its sub processors



# Compliance Packages

## Standard Contractual Clause (SCC) Outline Responsibilities

### Appendix 1

- Outlines the jurisdictions where the data is being processed
- Completed by the Data Exporter

### Appendix 2

- Defines data exporter and data importer
- Details categories of data to be transferred



# Compliance Packages

A man with grey hair and a beard, wearing a white dress shirt and a dark tie, is seated at a wooden desk. He is looking down at a tablet computer in his left hand while holding a pen in his right hand, ready to write on a notepad. The background is a bright, out-of-focus office environment.

## Standard Contractual Clause (SCC) Outline Responsibilities

### Appendix 3:

- Security measures of the data importer
- Often referred to as a Data Transfer Agreement (DTA)
  - Physical Access
  - Access control to data processing systems
  - Access control to specific use areas of data processing systems
  - Disclosure control
  - Input control
  - Job control
  - Availability Control
  - Separation control



# Statutory Compliance Integration

Payroll's Last  
Mile Automates



# Highly Manual & Complex

From hand writing payroll data on paper documents to requiring train trips to far-flung provinces to hand-deliver compliance paperwork

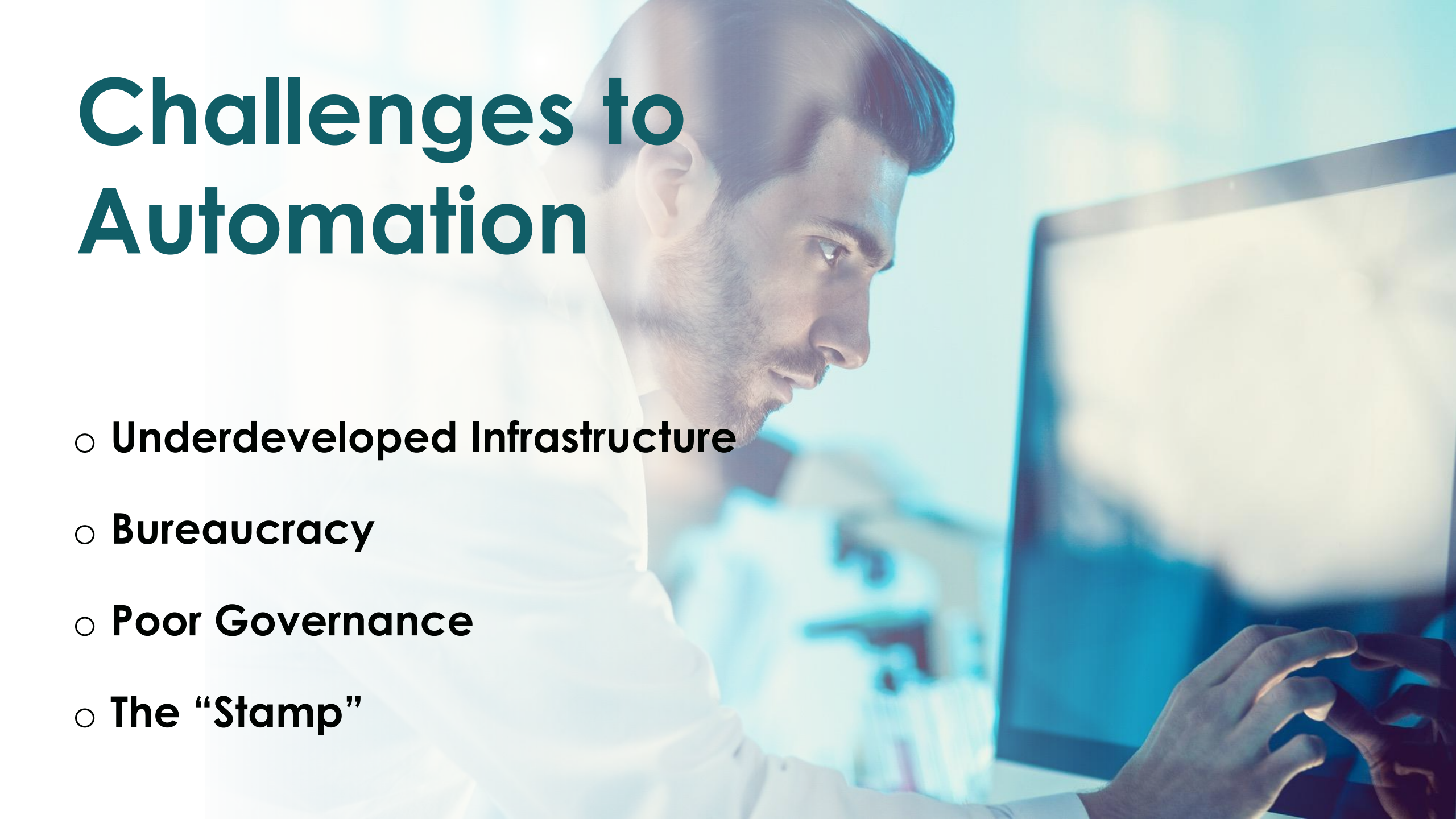
OR

# No Last Mile at All

Highly integrative from HRIS changes all the way through to online government filings



# Challenges to Automation

A man with dark hair and a beard, wearing a white shirt, is shown in profile, looking intently at a large computer monitor. The scene is bathed in a cool blue light, suggesting a modern office or laboratory environment. The monitor displays some indistinct, bright shapes. The overall mood is one of focused concentration and technological engagement.

- **Underdeveloped Infrastructure**
- **Bureaucracy**
- **Poor Governance**
- **The “Stamp”**



# Payroll's Last Mile Slowly Automates Why?

**Local Governments  
are looking to  
streamline Tax  
Reporting/Filing**

**Centralize & Standardize**

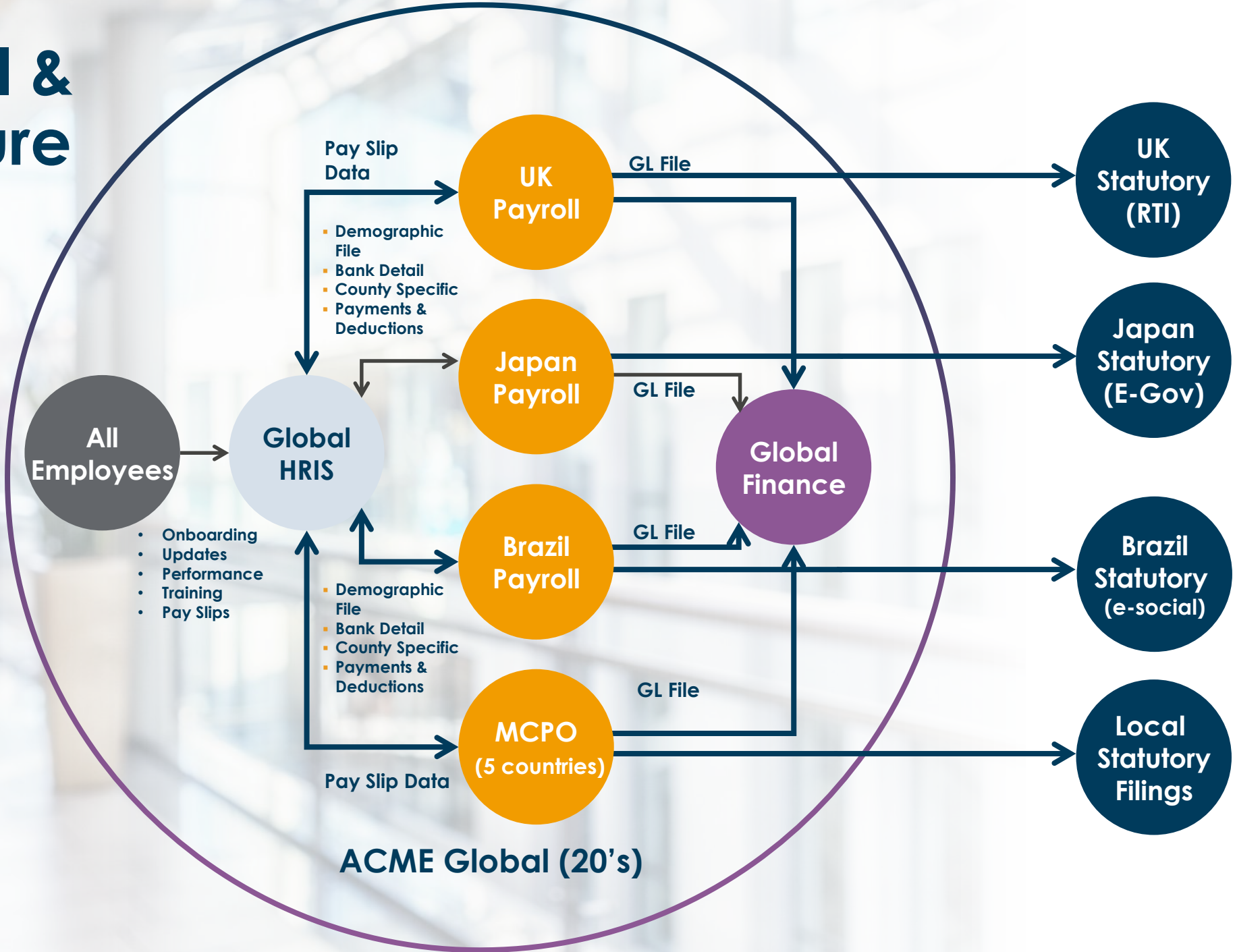
**Growing  
need for real  
time  
information**

**Reduce  
red tape**

**Reduce  
manual  
processes**



# HCM, Payroll & Finance Future Landscape





# Where is this Happening?

## Payroll Software Synced with Government Authorities

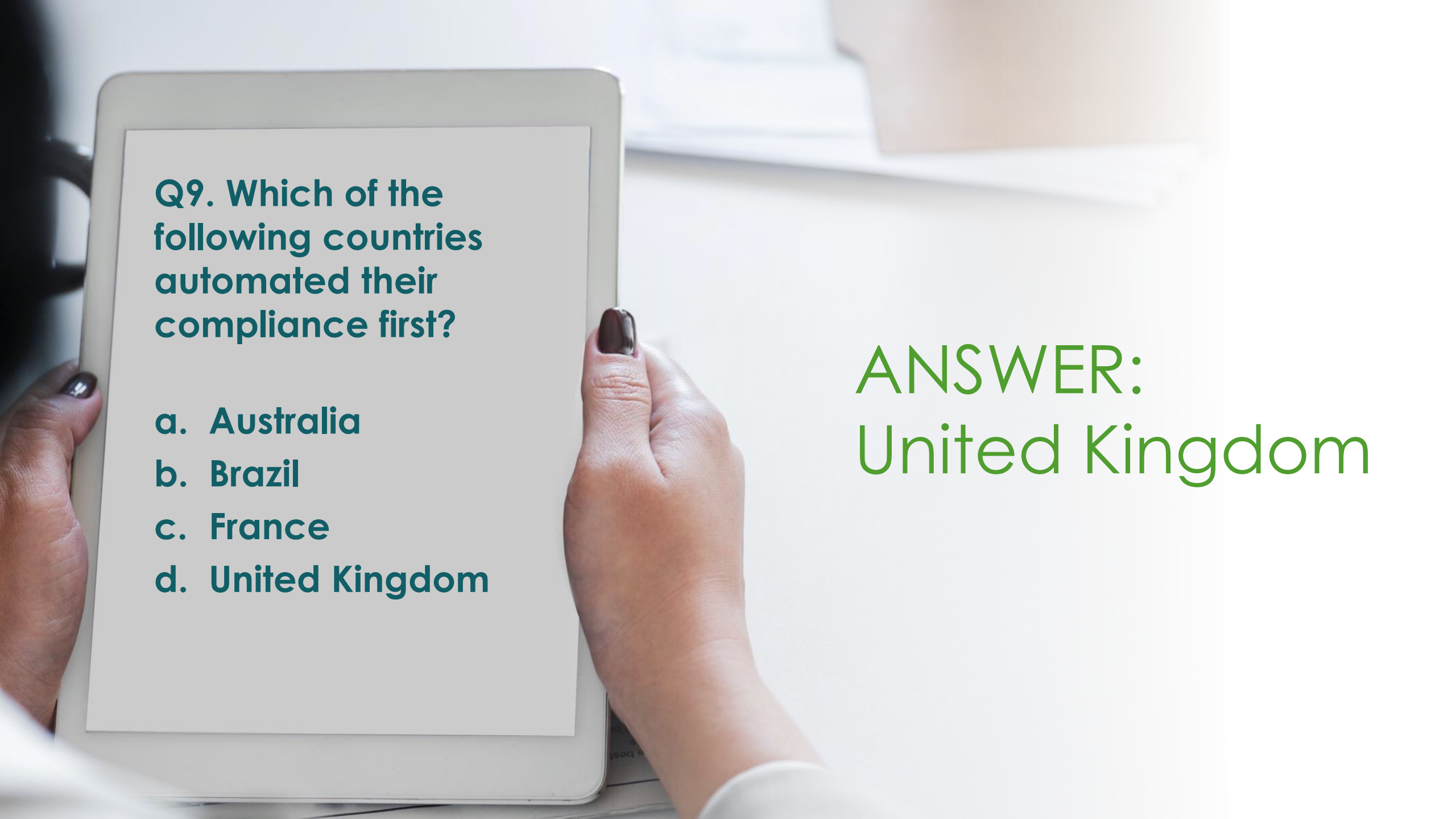
United Kingdom - Real Time Information (RTI)

France - Déclaration Sociale Nominative (DSN)

Brazil - E Social

Australia – SuperStream & Single Touch Payroll



A person's hands are visible holding a white tablet. The tablet screen shows a quiz question in dark teal text. The background is a bright, out-of-focus office setting with a desk and some papers.

**Q9. Which of the following countries automated their compliance first?**

- a. Australia**
- b. Brazil**
- c. France**
- d. United Kingdom**

**ANSWER:**  
**United Kingdom**



# UK Real Time Information (RTI)

## Real Time Information:

- Required by October 2013
- Provide data directly to the HMRC after each payroll run versus at the end of the year
- No longer will companies need to submit P14, P35, P38A or P45s to the HMRC
- Companies still need to submit P60's, P9D, P11D forms

# France DSN



## Déclaration Sociale Nominative:

**DSN automates the manner in which all Social Declarations are filed:**

- a. Employee Hires: (Fixed term, must provide end date of contract)
- b. Medical Leave: (Send within 3 days after leave to record for sickness, maternity, and paternity.)
- c. Leaving of an Employee: (Send within 3 workdays before the leave date)
- d. Monthly Changes: (Provide bonuses/premiums with dates of execution)
- e. Other Impacts: Employees on parental/sabbatical leave need a pay slip

**Required by January 2016**




# Brazil eSocial



## Goals of eSocial:

- Gradually replace obligations like CAGED, RAIS, SEFIP and GFIP (labor and social security withholding forms)
- Streamlines data sent to the government regarding payroll, labor, social security and tax obligations, and other information
- Ensures social security and labor rights are guaranteed for workers
- Simplifies compliance with obligations
- Improves the quality of information sent
- Employer obligations are not changing, they are just being submitted in a standard, consolidated, automated format

**Go live date moved from  
September 2016 to January 2018**

A person's hands are visible holding a white tablet. The tablet screen shows a quiz question and four multiple-choice options. The background is a blurred office desk with papers and a laptop.

**Q10. Which country  
has an automation  
technology called  
SuperStream?**

- a. United Kingdom**
- b. South Africa**
- c. Australia**
- d. Hong Kong**

**ANSWER:**  
**Australia**



# Australia SuperStream & Single Touch Payroll

## Goals of SuperStream:

- Automation of Superannuation payments by employers
- Employee must provide details of his or her selected pension program
- Standard interface for all programs
- All companies must comply by June 30, 2016

## Goals of Single Touch Payroll

- Employers need to report all payments, taxes and superannuation payments at the same time as employees are paid.





# Other Countries

- Japan's My Number
- Russian Data Localization
- China's Data Privacy 2018
- Others to follow....





# Thank You



**Pamela Webb**

**Senior Director,  
Global Strategy  
Ultimate Software**

**[pamela\\_webb@ultimatesoftware.com](mailto:pamela_webb@ultimatesoftware.com)**



**Michele Honomichl**

**Founder, Executive Chairman and  
Chief Strategy Officer  
Celergo**

**[mhonomichl@celergo.com](mailto:mhonomichl@celergo.com)**