

ASA
American Staffing Association

Navigating Data Security Requirements for International Operations

ASA *Pro*
WEBINARS

March 28

ASA
American Staffing Association

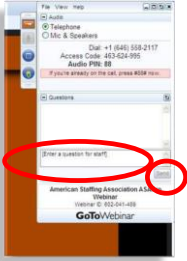
Brought to You by the


ASA TECHNICAL,
IT, & SCIENTIFIC
SECTION

ASA
American Staffing Association

How to Ask a Question




- Questions Panel
 - Type your questions into the Questions panel and click Send.




 American Staffing Association

How to Submit Your Legal CE for This Webinar


- Visit the ASAPro home page at americanstaffing.net/asapro.
- Log in to your ASAPro account.
- Click on CE Submission Form.




Navigating Data Security Requirements for International Operations

Bart A. Lazar, CIPP
Seyfarth Shaw LLP

 **Goals of Presentation**

- Foundation principles of information privacy and security
- How those principles are codified in federal and state laws
- Practical impact on staffing company operations
- Focus on international transfers of applicant data


6 | ©2013 Seyfarth Shaw LLP



What is Data Privacy/Security

- Not traditional “right to privacy”
—US v. Jones (installing a GPS system in a vehicle constituted a “search” under the fourth amendment).
- Individual’s right to ensure that personal data is not misused


7 | ©2013 Seyfarth Shaw LLP



What Information?

- Depends on the law involved
- Personal information, such as your name, address, telephone number, and email address online via our websites
- International laws
- US security breach laws—personal information
- Hipaa-Protected health information


8 | ©2013 Seyfarth Shaw LLP



What Information-EU?


- ‘Personal data’ shall mean any information relating to an identified or identifiable natural person (‘data subject’); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity

9 | ©2013 Seyfarth Shaw LLP

 **What Information-Canada?**


- “Personal information” means “information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization.”
- “Identifiable individual” where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other information
- Information need not be recorded
- Is intended to be interpreted broadly

10 | ©2013 Seyfarth Shaw LLP

 **What Information-State?**

- An individual's first and last name or last name or first initial and last name **COMBINED WITH:**
 - (a) Social Security number; or
 - (b) driver's license number or state-issued id card number; or
 - (c) financial account/credit/debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account.

11 | ©2013 Seyfarth Shaw LLP

 **Personal Information Is NOT**

- Information collected from publicly available sources or from federal, state or local government records
- E-mail address, whether or not combined with an individual's name
- Social Security Number, not connected with name (remember other state SSN laws-e.g. NY, CT, MI)
- Business contact information (in the US)

12 | ©2013 Seyfarth Shaw LLP

Why Do We Care?

- For many companies, collecting sensitive consumer and employee information is an essential part of doing business. If you collect this type of information, it's your legal responsibility to take steps to properly secure or dispose of that data.-Federal Trade Commission
- Protect company and clients

13 | ©2013 Seyfarth Shaw LLP

Why Do We Care?

- FTC/AG enforcement
- Costs associated with data security breaches
- Class-action law suits
- Goodwill

14 | ©2013 Seyfarth Shaw LLP

UNDERSTANDING THE INFORMATION ECOSYSTEM

```
graph TD; Company[Company] --- Clients[Clients]; Company --- Applicants[Applicants]; Company --- ServiceProviders[Service Providers]; Company --- Employees[Employees];
```

15 | ©2013 Seyfarth Shaw LLP



Information Protection- Applicants



- Administrative, technical and physical safeguards to protect against loss, misuse or unauthorized access, disclosure, alteration or destruction of information you provide on our websites

16 | ©2013 Seyfarth Shaw LLP




Information Collection- Employees

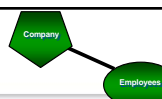


- Employees' personal information is collected as part of employment
- Employees are being given rights which are the equivalent to the rights of customers to their information
- Rights exist under International, U.S. and State laws and regulations

17 | ©2013 Seyfarth Shaw LLP



Information Protection- Employees



- Employees are tasked with the responsibility of meeting the company's privacy promises
- Customer and employee information must be protected by employees!
- Employees need training on their responsibilities (required under HIPAA and MA law)

18 | ©2013 Seyfarth Shaw LLP

Information Protection-Service Providers

- Service providers are given information by the company
- Service provider must use information only for company
- Agreement between service provider and company governs relationship
- Information is in control of company

19 | ©2013 Seyfarth Shaw LLP

Information Protection-Service Providers


- What to Put in Contract?
 - Broad representation regarding maintaining safeguards/compliance with applicable laws (minimum, but is it enough anymore?)
 - Specifically require encryption
 - Specifically require notifications (security breach)
 - Indemnification and control (practical)
 - March 2012-MA law- implement and maintain appropriate security measures for personal information

20 | ©2013 Seyfarth Shaw LLP

Information Protection-Clients

- Clients are permitted to use company information for their own business purposes
- Relationship determined by contract
- Clients have their own privacy policies and compliance obligations.


21 | ©2013 Seyfarth Shaw LLP



U.S. Privacy Principles

- Notice
- Choice
- Access
- Security


22 | ©2013 Seyfarth Shaw LLP



ADDITIONAL EU PRINCIPLES

- Onward transfer
- Data integrity
- Enforcement


23 | ©2013 Seyfarth Shaw LLP



Federal Laws

- FTC- Section 5- Unfair and Deceptive Trade Practices
- HIPAA/Hitech- Health Privacy/Security
- Sarbanes-Oxley-Security Re: Financial Controls
- FCRA/FACTA-Employee/Consumer Privacy
- GLB- Financial Privacy
- COPPA –Children’s On-Line Privacy
- ECPA- Communications Privacy

24 | ©2013 Seyfarth Shaw LLP



State Privacy Laws

- Database Security Breach (46 states, DC, PR and VI)
- Social Security Number
 - Protection
 - Policy Requirement
- Privacy Policy
- Encryption
- Reasonable Security Measures
- Detailed Security Measures (MA)


25 | ©2013 Seyfarth Shaw LLP



International Laws

- Applies to transfers of data to the United States
- Need consent, contract (even between affiliated companies) or other means of compliance
- US/EU Safe Harbor (certification to US govt. of compliance, not compliance in and of itself)

26 | ©2013 Seyfarth Shaw LLP



Compliance Choices For Data Transfers From The EU To Third Countries

- EU/US safe harbor rules
- EU standard clauses
- Alternative business clauses
- Ad-hoc data transfer agreements
- Binding corporate rules


27 | ©2013 Seyfarth Shaw LLP



WHY SECURITY?

- Identity theft is the number one crime
- Over 15,000,000 victims (every 2 seconds!)
- Record numbers of security breaches
- In last 7 years, there were 3665 publicly reported breaches—1.5/day


28 | ©2013 Seyfarth Shaw LLP



Applicant Data Breach Examples

- Plainfield, Illinois School District
 - Online Job Applications—www.applitrack.com
 - 23,000 individuals
 - 14 year old
- York County, SC
 - 17,000 job applicants
- Washington University, MI
 - Employee copying files
 - 4,100 employees and applicants


29 | ©2013 Seyfarth Shaw LLP



Sources of Security Breach

- Laptops/devices—theft/loss
- Employee conduct (intentional and negligent)
- Improper destruction
- Hacking
- “Glitch” or vulnerability
- Service provider

30 | ©2013 Seyfarth Shaw LLP

 **WHAT ARE REASONABLE MEASURES?**

- Assess
- Make your own determination
- Implement
- Train
- Evaluate

31 | ©2013 Seyfarth Shaw LLP

 **ADMINISTRATIVE SAFEGUARDS**

- Develop a security process
- Assign responsibility
- Limit access
- Security awareness and training
- Incident response plan
- Contingency plan
- Evaluation
- Contracts

32 | ©2013 Seyfarth Shaw LLP

 **PHYSICAL SAFEGUARDS**


- Facility access controls
- Limit workstation use
- Workstation security
- Device and media controls

33 | ©2013 Seyfarth Shaw LLP

 **TECHNICAL SAFEGUARDS**

- Access controls
- Audit controls
- Data integrity
- Authentication
- Transmission security
- System monitoring
- Firewall protection

34 | ©2013 Seyfarth Shaw LLP

 **State Database Security Breach**


- Personal information
- Electronic (except MA and NC)
- Unauthorized use or disclosure (some exceptions)
- Now also HIPAA

35 | ©2013 Seyfarth Shaw LLP

 **INTERNATIONAL TRANSFER-Not for US Employers**


- Age
- Race
- Religion
- Disability
- National origin
- Gender
- Familial status
- Sexual orientation

36 | ©2013 Seyfarth Shaw LLP

 **INTERNATIONAL TRANSFER-Not for US Employers**


- No laws forbidding employer from receiving
- Good practice for employer to not receive
- Administrative procedure to review and scrub is a best practice

37 | ©2013 Seyfarth Shaw LLP

 **Database Security Breach Notifications**


- Notice to owner of data (if a vendor/service provider)
- Individuals/consumers
- Regulators (HHS, if it involves PHI and more than 500 individuals)
- Consumer reporting agencies
- Law enforcement

38 | ©2013 Seyfarth Shaw LLP

 **WHEN DOES A “BREACH” REQUIRE NOTIFICATION?**

- Depends on the state
- Unauthorized “acquisition”
- Unencrypted data (or encrypted with key-ma)
- Compromises security, confidentiality or integrity of personal information

39 | ©2013 Seyfarth Shaw LLP

 **CAN A “BREACH” BE CURED?**


- Depends on the state
- Appropriate investigation
- Consultation with law enforcement
- Determination of no reasonable likelihood of harm to consumers
- Misuse has not occurred/unlikely to occur
- Notice to AG

40 | ©2013 Seyfarth Shaw LLP

 **Questions?**

Bart A. Lazar:
(312) 460-5986
blazar@seyfarth.com

41 | ©2013 Seyfarth Shaw LLP

 **ASA**
American Staffing Association

Thank You for Attending

- Today's webinar has been recorded.
- Recording will be available within three days.



American Staffing Association

Upcoming Webinars

- April 11: Tips on Submitting ASA Award Entries: Care, VOICE, and National Staffing Employee of the Year
- April 18: Conducting Harassment Investigations With Clients

This ASAPro webinar qualifies for 1.0 legal active CE hour



American Staffing Association

STAFFING[®] WORLD
2013
Oct. 8-10 • Orlando
ASA Convention & Expo

Registration is now open for the premier staffing event of the year—the ASA annual convention and expo.

Go to staffingworld.org today to start planning your Staffing World 2013 experience, and to register at the lowest rate available!

The Can't Miss Event for Staffing Executives
