Breakout Sessions – Series 4

MANAGING EMPLOYEE DATA PRIVACY

A WORLDWIDE STRATEGY FOR MULTINATIONAL EMPLOYERS

Bonnie Puckett (Moderator) – Ogletree Deakins (Atlanta)

Simon J. McMenemy – Ogletree Deakins (London)

Grant D. Petersen – Ogletree Deakins (Tampa)
Overview

Multinational companies must comply with a myriad of U.S. and international data privacy laws regarding human resources data. Since the EU General Data Protection Regulation became effective in May 2018, several countries including the U.S. have implemented or updated their data privacy laws to provide for stricter privacy rights for employees and applicants. Consequently, multinational employers should monitor and keep apprised of the rapidly changing data privacy laws in the countries in which they employ employees and develop a strategy for implementing a worldwide data privacy compliance program.

EU Developments

Much has happened since the European Union (EU) General Data Protection Regulation (GDPR) went into effect on May 25, 2018. Many EU countries have enacted national legislation to implement and expand the requirements of the GDPR, while other developments have directly affected employers and created new obligations regarding the collection and processing of human resources (HR) data. Further, several EU supervisory authorities have issued significant civil penalties for GDPR violations. The key developments for employers are as follows:

Country-Specific Requirements for HR Data

Although the GDPR was intended to provide a uniform set of data protection requirements across the EU, the GDPR contains several provisions, known as “opening clauses,” that expressly permit individual EU countries to implement additional and/or stricter requirements for certain types of data that employers typically process. For example, Article 9 of the GDPR provides that EU Member States may introduce further conditions and limitations on the processing of genetic data, biometric data, and health data. Article 10 of the GDPR provides that data concerning criminal convictions and offenses may be processed only if authorized by EU or EU country law. Finally, Article 88 permits EU countries to provide, either by law or by collective agreements, more specific rules regarding the processing of personal data in the employment context.

Several EU Member States have taken advantage of these opening clauses and have enacted legislation providing stricter or additional requirements for processing HR data. Examples of these requirements include:

- **Denmark**
  - All organizations, including employers, must encrypt emails that contain sensitive personal data. “Sensitive personal data” under the GDPR includes data concerning a person’s racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic information, biometric data ideology, union membership, sexual orientation, beliefs, or health, sex life, or sexual orientation.

- **France**
  - Private-sector employers are prohibited from processing criminal history data as such data may be processed solely by public entities or in connection with legal proceedings.
Employers may process biometric data if such processing is strictly necessary to control access to the workplace and devices and applications used by employees, agents, trainees, or service providers.

- **Germany**
  - An employer must appoint a data privacy officer if it employs 10 or more people whose duties include the processing of personal data.
  - An employer may engage in employee monitoring only when the company can document reasons to believe the employee is engaged in criminal conduct or has or is committing a serious breach of duty.

- **Poland**
  - Employers may not process the criminal histories of job applicants, even with applicant consent.
  - Employers may not contact the prior employers of job applicants without the applicants’ consent.
  - Employers may not confirm the authenticity of job applicants’ university degrees.
  - Employers may not retain the data of unsuccessful job applicants for future employment consideration unless the job applicants consent.
  - Employers may not process job applicants’ social media data.

- **Spain**
  - Employers cannot process criminal record data unless specifically permitted by a sector law.
  - An employer must notify employees of any video surveillance by placing a sign regarding the surveillance in a visible location. Video surveillance data must be deleted within one month unless needed to prove the commission of acts against individuals, property, or facilities.
  - Employers may access corporate electronic devices used by employees pursuant to clear rules drafted with the participation of the workers’ representatives. However, employees have the right to disconnect from company networks outside of working hours in accordance with predefined policies.
  - Employers cannot process criminal record data unless specifically permitted by a sector law.

- **United Kingdom**
  - Employers are not required to provide employees or job applicants access to confidential references provided for employment purposes.
  - Employers may process criminal history data only if one of the following conditions is met: “the data subject has given consent to the processing”; “the processing is necessary to protect the vital interests of an individual”; the processing is performed by a not-for-profit entity; the “personal data is already in the public domain”; “the processing is necessary for the purpose of, or in connection with, any legal proceedings” or is necessary for obtaining legal advice or establishing, exercising, or defending legal rights; “the processing is of personal data about a conviction or caution” for an indecency offense involving children; the processing is “necessary for reasons of substantial public interest”; or the processing is necessary for insurance purposes.
Employers Must Conduct DPIAs

Article 35 of the GDPR provides that a data protection impact assessment (DPIA) must be performed for data processing that “is likely to result in a high risk to the rights and freedoms of natural persons.” DPIAs must contain (1) a description of the processing operation along with the purpose of the processing and, where applicable, the legitimate interest for the processing; (2) an assessment of the necessity and proportionality of the processing operation in relation to the purpose; (3) an assessment of the risks to the rights and freedoms of the data subjects; and (4) the measures to be taken to mitigate the risks. Article 35 of the GDPR also requires the supervisory authority of each EU country to submit a list of the kind of processing for which a DPIA must be performed (a so-called “blacklist”) to the European Data Protection Board (EDPB) for review and recommendations.

During 2018, the EDPB issued opinions regarding the draft lists submitted by each EU country. In its opinions, the EDPB attempted to harmonize the criteria for conducting DPIAs across all EU countries and provided recommendations regarding the need for a DPIA for several types of data processing. Specifically, the EDPB made the following findings and recommendations:

- Criteria for DPIAs: The EDPB recommended that each country make reference to and follow the Working Party Guidelines regarding DPIAs and to require DPIAs if any two of the following nine criteria were present: (1) evaluation or scoring (which would include employee performance evaluations and applicant evaluations); (2) automated decision making; (3) systematic monitoring; (4) sensitive data or data of a highly personal nature; (5) data processing on a large scale; (6) matching or combining data sets; (7) processing data of vulnerable subjects, which include children, the elderly, and employees; (8) innovative use or application of technological or organizational solutions, such as using fingerprints or facial recognition for physical access control; and (9) processing that “prevent[s] data subjects from exercising a right or using a service or a contract.”

- Non-Exhaustive Nature of the Lists: The EDPB stated that each country should indicate that its list is not to be considered exhaustive.

- Employee Monitoring: The EDPB stated that each country should indicate that a DPIA must be performed when an employer engages in systematic monitoring of employees. The EDPB stated that the Working Party’s June 8, 2017, Opinion on data processing at work remains valid in defining when systematic monitoring of employees occurs. The Working Party’s Opinion requires or recommends that a DPIA be performed for the monitoring of employee computer, email, and mobile device usage; monitoring employees for time and attendance; monitoring employees through video surveillance; monitoring employees for access control; and monitoring location and vehicle use data.

- Biometric Data: The EDPB stated that each country should indicate that a DPIA must be performed for the processing of biometric data for the purpose of uniquely identifying a natural person so long as at least one of the nine criteria is present.
• Genetic Data: Similarly, the EDPB stated that each country should indicate that a DPIA must be performed for the processing of genetic data so long as at least one of the nine criteria is present.

• Location Data: The EDPB also stated that each country should indicate that a DPIA must be performed for the processing of location data so long as at least one of the nine criteria is present.

• Migration of Data: The EDPB stated that each country should indicate that a DPIA should be performed when data is migrated from one system to another and at least one of the nine criteria is present.

Significantly, the EDPB stated that DPIAs should not be performed for cross-border data transfers or data processed by joint controllers (for example, HR data of EU employees processed by both an EU subsidiary and U.S. parent company) and instructed applicable countries to remove such processing from their lists.

Based on the EDPB opinions, employers must perform DPIAs for any monitoring of employees located in the EU. Also, because employees are considered to be vulnerable subjects, the processing of HR data will always meet at least one of the criteria that trigger the need to perform a DPIA. Thus, employers will be required to perform DPIAs for data processing involving biometric data, genetic data, location data, and the migration of data as well as data processing involving the one of the following criteria:

• Employee and job applicant evaluations.
• Automatic decision making, such as the use of algorithms in online job applications that screen applicants without the need for human intervention.
• Sensitive data such as racial and ethnic background, trade union membership, religious beliefs, and employee health data.
• Innovative technology such as the use of fingerprints or facial recognition for access control.

**Brexit**

Companies should consider taking provisional steps to mitigate any impact to their data transfers if there is a “no deal” Brexit. They may also need to appoint data protection representatives in the United Kingdom and/or the European Union.

After Brexit, the European Union will treat the United Kingdom as a “third country”. The GDPR prevents EU entities from transferring personal data to third countries unless the EU Commission has granted an “adequacy decision” (establishing that the data protection regime of the destination is “essentially equivalent” to that of the European Union), the parties use an approved data transfer mechanism or an exception in the GDPR applies.

The United Kingdom’s position on data protection is to maintain a close alignment with EU data protection laws and seek an adequacy decision to avoid disruption to data flows. However, an adequacy decision will only apply as part of an agreed Brexit and not as part of a “no deal” Brexit. The EU Commission has said that EU companies making transfers of personal data to the United Kingdom after a “no deal” Brexit must rely on the available transfer mechanisms under the GDPR.
U.S. Developments

Privacy Shield

At the end of 2018, the European Commission issued its second annual review of the performance of the 2016 EU-U.S. Privacy Shield. The report was generally very positive, with the commission noting that the Privacy Shield continues to ensure an adequate level of protection for personal data transferred from the EEA to Privacy Shield-compliant companies in the U.S.

The Department of Commerce (“DoC”) has provided companies who self-certify to the Privacy Shield with some guidance on how to handle U.K. data in light of Brexit. Given the uncertainty surrounding Brexit, the DoC outlined two potential scenarios:

- **Transition Period Scenario**: The U.K. and EU have agreed that there will be a transition period ending December 31, 2020, during which EU law, including EU data protection law, will continue to apply in the U.K. During this period, the Privacy Shield will continue to apply to data transfers from the U.K. to U.S. Privacy Shield participants and no additional action will be required of Privacy Shield participants.

- **No Transition Period Scenario**: If there is no transition period, then the steps outlined below need to be in place by March 29, 2019 (assuming no delay in the Brexit date). Steps that will be required to import U.K. data under the Privacy Shield:

  - All public notices regarding the Privacy Shield explicitly must state that personal data received from the U.K. is in reliance on the Privacy Shield. Human resource policies also must be updated if HR data is imported from the U.K. in reliance on the Privacy Shield.

  - The Department of Commerce has provided the following model language to be used in the public notices:

    \[
    \text{(INSERT your organization name) complies with the (INSERT EU-U.S. Privacy Shield Framework [and the Swiss-U.S. Privacy Shield Framework(s)]) (Privacy Shield) as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the (INSERT European Union and the United Kingdom and/or Switzerland, as applicable) to the United States in reliance on Privacy Shield. (INSERT your organization name) has certified to the Department of Commerce that it adheres to the Privacy Shield Principles with respect to such information. If there is any conflict between the terms in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification, please visit https://www.privacyshield.gov/).}
    \]

California Consumer Privacy Act

On January 1, 2020, the California Consumer Privacy Act (CCPA) becomes effective. Although the law provides that it is applicable to “consumers,” the definition of “consumer” is
broad enough to include employees so long as they are natural persons who are California residents. In any event, employees will be covered if they are also consumers of the company. The key issues for employers regarding the CCPA are as follows:

- **Coverage**

  With some exceptions, employers must comply with CCPA if they receive personal information from California residents (including employees) and if their business, subsidiary or parent company meets at least one of the following criteria:

  - Has annual gross revenues of $25 million;
  - Buys, receives, sells, or shares the personal information of 50,000 or more California consumers, households, or devices annually for commercial purposes (whether alone or in combination with others); or
  - Derives at least 50% percent of its annual revenues from selling California residents’ personal information.

- **Personal Information**

  The CCPA defines personal information as “any information that . . . relates to . . . a particular consumer or household” and specifically includes professional or employment-related information.

- **Employer Obligations**

  Employers will be required to implement internal and external processes and data handling practices to effectuate employee rights under the CCPA such as updating employee privacy policies and/or notices, creating or revising data maps and/or data inventories, revising contracts with service providers, and creating a data access request procedure.

- **Employee Rights**

  California consumers and covered employees will have the following rights:

  - Employees must be informed about the categories of personal information collected and the purpose of the collection at or before the time of collection.
  - No additional categories of information can be collected without prior notice.
  - Employees must be informed if their personal information is being sold or disclosed to third parties for “business purposes” that include disclosures to payroll vendors, benefit providers, and others.
  - Employers need to ensure their agreements with service providers prohibit any sale or unauthorized use of employee information other than specified processing purposes.
  - Employees cannot contractually waive any rights provided by the CCPA.
  - Employees must be notified of and may exercise their CCPA rights by using toll-free numbers for submitting requests and clear and conspicuous links titled “Do Not Sell My Personal Information.”
  - Employees may request that employers disclose the categories of personal information collected about them and the specific personal information collected.
Employers must provide the information free of charge within 45 days once the request is verified (with a limit of no more than two requests per 12-month period).

- Employees can request that their personal information be deleted. However, employers are permitted to retain the information necessary for performance of the employment contract or it is required only for internal purposes related to security, First Amendment rights, and other purposes detailed in Cal. Civ. Code § 1798.105(d) et seq.
- Employees have the right to opt out of the “sale” of their personal information.
- An employer cannot retaliate or discriminate against employees who exercise their rights under CCPA.

Other International Developments

Brazil

- Coverage

The Law governs processing of personal data in Brazil including the collection, storage, transfer, deletion and other activities related to personal data. The Law applies to any processing of personal data that:

- Occurs in Brazil
- Offers goods or services in Brazil
- Applies to individuals who were in Brazil when data was collected

- Personal data

Personal data is all information related to an identified or identifiable individual and includes among other things name, address, telephone number, ID number, Tax ID number, driver’s license, and bank account information.

- Legal Bases for Processing Personal Data

- The company obtains the data subject’s consent for processing personal data
- The company is a controller and processing personal data is required for compliance with a legal or regulatory obligation
- Data processing is required for performance of a contract, at the request of the data subject
- To exercise the company’s rights, whether arising from contract or in a court, administrative or out-of-court proceeding
- The company or third parties have a legitimate interest to process personal data
- For credit protection

- Processing sensitive data

Sensitive data is data includes an individual's racial or ethnic origin, religious beliefs, political opinion, trade union membership, health or sex life, and genetic or biometric data. If the company intends to process sensitive data, it must obtain the relevant data subject's specific consent, except when processing is indispensable for:
o Compliance with a legal or regulatory obligation
o Exercise of company rights arising from contract or in a court, administrative or out-of-court proceeding
o Security purposes to ensure fraud prevention

• Cross-Border Data Transfers

The transfer of data from Brazil to other countries may only occur if:

o The country of destination offers adequate protection to personal data
o There are standard contractual clauses between controllers and the recipient of personal data
o The company adopts binding corporate rules
o The company adopts approved data protection seals, certifications, and code of conduct
o The Brazilian Data Protection Authority authorizes the transfer
o The data subject has given specific and highlighted consent for the transfer

India

• Coverage

The Act applies to processing of personal data collected, disclosed, shared or otherwise processed within India. It also applies to data controllers and data processors outside India if processing is in connection with business carried out in India, or in connection with systematic offering of goods or services to data subjects in India, or in connection with activity that involves profiling of Indian data subjects. This would sweep in almost any entity with an Indian connection or which offers goods/services through a website in India for example.

• Personal data

Personal data is defined as data about or relating to a natural person. “Sensitive personal data” includes passwords, financial data, health data, sexual orientation, biometrics, and caste data, but this is not an exhaustive list. However, the Act excludes “irreversibly” anonymized data from its requirements.

• Legal Bases for Processing

Processing of both personal data requires a lawful processing basis. Consent is a lawful basis for both personal data and sensitive personal data, but heightened information requirements apply for sensitive personal data. The Act permits data to be processed for a purpose “reasonably incidental” to the purpose for which it was collected. It also permits processing for “a reasonable purpose.”

• Notice Requirements

The Act requires data controllers to provide notice to data subjects regarding data processing.
• **Data Subject Rights**

Data subjects have the right to confirmation of data and access to data, data portability, right to be forgotten, as well as the right to correction of the data. The “right to be forgotten” requires a data subject to submit a request to an adjudicating authority under the Act, which weighs the request against various other factors before deciding whether to grant it.

• **Data Residency Requirements**

A copy of all personal data subject to the Act must be stored in India by the data controller but additional copies can be stored outside India.

• **Cross-Border Data Transfers**

Cross border data transfers are permitted only through:

  o standard contractual clauses approved by the Data Protection Authority under the Act; or
  o EU style adequacy decisions from the Indian government.

Additional consent of the data subject may be required, though it is unclear from the Act whether this is still needed if using one of the mechanisms above.

• **DPIAs**

The Data Protection Authority can classify data controllers as “significant” or high risk if they process large volumes of personal data, process sensitive personal data, and depending on turnover, risk of harm to data subjects, and a number of other factors. Such data controllers must conduct data protection impact assessments (DPIAs), comply with record keeping requirements, conduct data audits, and appoint a Data Protection Officer.

• **Data Breach Notification**

Data controllers must notify the Data Protection Authority as soon as possible of any breach where the “breach is likely to cause harm to any data subject.” The Data Protection Authority then determines if data subjects must be notified.

**China**

The Cyber Security Law, which became effective on June 1, 2017, applies to personal data collected over information networks.

• **Coverage**

The Cyber Security Law imposes data privacy obligations on network operators. The term “network operator” includes both owners and administrators of a network as well as network service providers. A “network” is defined as any system that consists of computers or other information terminals, and related equipment for collecting, storing, transmitting, exchanging and processing information.
• **Personal Data**

Personal data is defined as information that identifies a natural person either by itself or in combination with other information. The term includes a person’s name, address, telephone number, date of birth, identity card number and biometric identifiers. Sensitive personal data is defined as personal data that, if disclosed or illegally processed might endanger personal and property security, damage personal reputation, or physical or psychological health, or lead to discriminatory treatment, etc. Sensitive personal data may include personal ID card numbers, biometric data, bank account numbers, personal communications, credit records, geolocation data and health data, as well as the personal data of children under the age of 14 years.

• **Data Collection and Processing**

Network operators are prohibited from collecting personal data that is not relevant to the services they offer. Prior to collecting personal data from a data subject, a network operator is required to explicitly inform the individual of the purposes, means and scope of the collection and use of their data, and obtain their consent for collection. Any processing of personal data must be done in accordance with the scope of those consents. It is unclear whether the same standards are intended to apply to employee information. However, the definition of a “network” is certainly wide enough to include internal systems, as noted above.

• **Storage and Security**

Network operators must keep data subjects’ personal data in strict confidence, must implement technical measures to monitor and record the operational status of their networks and the occurrence of cyber security incidents. Network operators are also required to back up and encrypt “important data,” and store operations logs for at least six months. “Important data” is data that is closely related to national security, economic development and societal and public interests.

• **Breach Notifications**

Network operators must promptly notify data subjects of a data breach or other loss of personal data. A network operator is also required to report the incident to the relevant sector regulator and to take immediate remedial action. The incident notification must describe:

- the nature and impact of the incident
- the measures taken or to be taken in response
- the practical recommendations for data subjects to minimize the impact of the incident on them, and
- the data subjects’ rights and remedies.

• **Data Transfers**

Network operators must obtain the informed consent of data subjects to transfer or disclose any of its personal data to a third party whether within or outside the country. To obtain consent, the network operator must first notify the data subject of:

- the type of personal data being transferred
- the purpose and scope of the transfer, and
- the recipient and the country to which the data will be transferred.
Network operators must conduct a security assessment on an annual basis before transferring any personal data out of China. The security assessment must take into consideration the following factors:

- the necessity of the overseas transfer
- the amount and sensitivity of personal data
- the security measures taken by the recipient
- the data protection legal environment in the recipient country
- the risk of a data breach
- whether the transfer includes “important data”
- the risks to national security, societal and public interests or personal legitimate interests.

Network operators must submit the security assessment report to the relevant authorities before making the transfer if:

- the network operator transfers the personal data of more than 500,000 individuals in aggregate in any one year
- any individual data transfer exceeds 1,000 gigabytes
- circumstances exist that could affect national security, economic development and societal and public interests.

- **Data Localization**

  All personal data and important data held by critical information infrastructure operators must be stored in China. Critical information infrastructure is defined as an information infrastructure that affects national security, the national economy and people’s livelihoods, such that, if data is leaked, damaged or loses its functionality, national security and public interests may be seriously harmed.

- **Data Subject Rights**

  Data subjects have the right of erasure, right of data portability, and right to appeal automated decisions that directly impact the rights and interests of a data subject.

**Key Takeaways for Employers**

Although multinational employers must comply with myriad of different data protection laws regarding their employees’ HR data, employers should adopt a worldwide strategy for compliance based on the following eight themes that are common among the data protection laws throughout the world:

- **Build Upon Your GDPR Compliance Program.** Most data protection laws, including the California law, are modeled after the GDPR. Thus, your GDPR compliance program should serve as the baseline program for global compliance.

- **Provide Detailed Notice.** Most data protection laws require detailed notices to data subjects regarding the processing of their data.
- **Accountability Documentation.** Be accountable for your data by documenting what you have, why you have it, where it is and what you are doing with it. Include all legal bases for processing. Conduct DPIAs for sensitive processing functions.

- **Compliance Documentation.** Document your data management and efforts at compliance to provide assurance to auditors, regulators and trading partners.

- **Breach Notification Readiness.** Be prepared to quickly investigation and give notice to data subjects, business partners and/or government authorities if a breach happens. Many countries have short notice periods.

- **Upgrade Data Security Programs.** Continue to upgrade your best practices for data security to stay ahead of emerging threats. Your upgraded program should include assigning qualified security staff to actively monitor systems and engage in strict access control, looking for clues that an intrusion has happened and disrupting attacks.

- **Self-regulation.** Regulate your own data security practices. Maintain an ongoing, well-resourced process for auditing and evaluating your data protection and improving it constantly.

- **Vendor Management.** Require your vendors to implement appropriate security measures to avoid the mishandling of your data and conduct regular audits.

- **Leadership.** Appoint responsible leadership for compliance. Designate a qualified person to lead your privacy and data protection team, and give that person the necessary budget and authority.
Managing Employee Data Privacy:
A Worldwide Strategy for Multinational Employers

Presenters
Simon McMenemy (London) and Grant Petersen (Tampa)

Moderator
Bonnie Puckett (Atlanta)

Multinational Employers Face a Myriad of
Data Protection Laws

- EU Developments
  - Evolving GDPR Requirements
  - Brexit
- U.S. Developments
  - Privacy Shield
  - California Consumer Privacy Act
- Other International Developments
- Need Worldwide Compliance Strategy
EU Developments – GDPR

- **Country-Specific Requirements**
  - **Denmark:**
    - Encrypt all emails containing sensitive data
  - **France:**
    - Private sector employers prohibited from processing criminal history data.
    - Employers may process biometric data if such processing is strictly necessary to control access to the workplace and devices.

EU Developments – GDPR

- **Country-Specific Requirements**
  - **Germany:**
    - Employers must appoint a data privacy officer if they employ 10 or more people whose duties include the processing of personal data.
    - Employers may engage in employee monitoring only when the company can document reasons to believe the employee is engaged in criminal conduct or has or is committing a serious breach of duty.
EU Developments – GDPR

- **Country-Specific Requirements**
  - **Poland:**
    - Employers may not process the criminal history of job applicants even with the applicant’s consent.
    - Employers may not contact the prior employer of a job applicant without the applicant’s consent.
    - Employers may not confirm the authenticity of a job applicant’s university degree.
    - Employers may not retain the data of an unsuccessful job applicant for future consideration of employment unless the job applicant consents.
    - Employers may not process a job applicant’s social media data.

- **Spain:**
  - Employers must notify employees of any video surveillance by placing a sign regarding the surveillance in a visible location.
  - Video surveillance data must be deleted within one month unless needed to prove the commission of acts against individuals, property, or facilities.
  - Employers may access corporate electronic devices used by employees pursuant to clear rules drafted with the participation of the workers’ representatives.
  - Employees have the right to disconnect from the company networks outside of working hours.
  - Employers cannot process criminal record data unless specifically permitted by a sector law.
EU Developments – GDPR

- **Country-Specific Requirements**
  - **United Kingdom:**
    - Employers not required to provide employees or job applicants access to confidential references provided for employment purposes.
    - Employers may process criminal history data if:
      - obtain consent
      - protecting the individual’s vital interests,
      - defending legal claims, or
      - necessary for insurance purposes.

EU Developments – GDPR

- **Prepare Required Data Privacy Impact Assessments (DPIAs)**
  - DPIA must be performed for data processing that “is likely to result in a high risk to the rights and freedoms of natural persons.”
  - Each EU country submitted DPIA list to EDPB for opinion
EU Developments – GDPR

- Criteria for DPIAs – any 2 present:
  - evaluation or scoring (which would include employee performance evaluations and applicant evaluations)
  - automated decision making
  - systematic monitoring
  - sensitive data
  - data processing on a large scale
  - matching or combining data sets
  - processing data of vulnerable subjects, which include employees
  - innovative use or applying technological or organizational solutions
  - processing that prevents data subjects from exercising a right or using a service or contract

EU Developments – GDPR

- DPIA must be performed for:
  - Employee monitoring
  - Processing biometric data
  - Processing genetic data
  - Location data
  - Migration of data
  - Employee and job applicant evaluations
  - Automatic decision making
  - Sensitive data
  - Innovative technology
EU Developments – Brexit

U.S Developments – Privacy Shield

- Second Annual Review – Privacy Shield Adequate
  - Standard contract clauses under attack
  - BCR best option but costly

- Brexit Revisions
  - Transition
  - No deal
U.S Developments – CCPA

**Coverage**
- Annual gross revenues of $25 million;
- Buys, receives, sells, or shares personal information of 50,000 or more California consumers; or
- Derives at least 50% of its annual revenues from selling California residents’ personal information.

**Employers as Consumers?**

U.S Developments – CCPA

**Personal Information**
- “any information that . . . relates to . . . a particular consumer or household” and specifically includes professional or employment-related information

**Employer Obligations**
- Implement internal and external data handling practices;
- Update employee privacy policies and/or notices;
- Create or revise data maps and/or data inventories;
- Revise contracts with service providers; and
- Create data access request procedure.
U.S Developments – CCPA

**Employee Rights**

- Informed about the categories of personal information collected and the purpose of the collection.
- No additional categories of information can be collected without prior notice.
- Informed if their personal information is being sold or disclosed to third parties for “business purposes.”
- Agreements with service providers prohibit any sale or unauthorized use of employee information.
- Employees cannot contractually waive CCPA rights.

**Employee Rights**

- Notified of and exercise CCPA rights by using toll-free numbers and links titled “Do Not Sell My Personal Information.”
- Request that employers disclose the categories of personal information collected about them and the specific personal information collected.
- Receive requested information free of charge within 45 days.
- Request that personal information be deleted. Employees have the right to opt out of the “sale” of their personal information.
- No retaliation for exercising rights.
Other International Developments – Brazil

- **Coverage**
  - Processing occurs in Brazil
  - Offers goods or services in Brazil
  - Applies to individuals who were in Brazil when data was collected

- **Personal data**
  - Identified or identifiable individual

Other International Developments – Brazil

- **Legal Bases for Processing Personal Data**
  - Consent
  - Compliance with a legal or regulatory obligation
  - Required for performance of a contract
  - Exercise the company’s rights in contract or legal proceeding
  - Legitimate interest to process personal data
  - For credit protection
Other International Developments – Brazil

- **Processing Sensitive Data**
  - Compliance with a legal or regulatory obligation
  - Exercise of company rights arising from contract or in a court, administrative, or out-of-court proceeding
  - Security purposes to ensure fraud prevention

- **Cross-Border Data Transfers**
  - Adequate protection to personal data
  - Standard contractual clauses
  - Binding corporate rules
  - Approved data protection seals, certifications, and code of conduct
  - The Brazilian DPA authorizes the transfer
  - The data subject consent for the transfer
Other International Developments – India

- **Coverage:**
  - Personal data collected or processed within India
  - For data controllers and data processors outside India:
    - Processing is in connection with business carried out in India
    - Systematic offering of goods or services to data subjects in India
    - Activity that involves profiling of Indian data subjects

- **Personal Data**
  - Data about or relating to a natural person
  - Sensitive data includes passwords, financial data, health data, sexual orientation, biometrics, and caste data

- **Legal Bases for Processing**
  - Consent
  - “A reasonable purpose"
Other International Developments – India

- **Data Subject Rights**
  - Confirmation of data and access to data
  - Data portability
  - Right to be forgotten
  - Correction of the data personal data

- **Data Residency Requirement**

- **Cross-Border Data Transfers**
  - Standard contractual clauses
  - Adequacy decision

Other International Developments – India

- **DPIAs**
  - Classify data controllers as "significant" or high risk if:
    - Process large volumes of personal data
    - Process sensitive personal
    - Risk of harm to data subjects

- **Data Breach Notification**
  - “Likely to cause harm to any data subject”
  - Notify the DPA ASAP
  - DPA determines if notice needed for data subjects
Other International Developments – China

- **Coverage**
  - Network operators
  - Network is a system that consists of computers or other information terminals for collecting and processing information

- **Personal Data**
  - Identifies a natural person
  - Sensitive personal data is data that would cause harm if disclosed

- **Data Collection and Processing**
  - Process relevant information only
  - Notice and consent required

- **Storage and Security**
  - Keep personal data in strict confidence
  - Implement technical measures to monitor and record the operational status of networks and the occurrence of security incidents
  - Back up and encrypt “important data”
Other International Developments – China

- **Breach Notifications**
  - Promptly notify data subjects
  - Report incident to the relevant sector regulator
  - Take immediate remedial action

- **Data Transfers**
  - Obtain consent
  - Notify the data subject of:
    - Type of personal data being transferred,
    - Purpose and scope of the transfer, and
    - Recipient and the country to which the data will be transferred.

Other International Developments – China

- Conduct annual security assessment based on:
  - Necessity of the overseas transfer
  - Amount and sensitivity of personal data
  - Security measures taken by the recipient
  - Data protection legal environment in the recipient country
  - Risk of a data breach
  - Transfer includes “important data”
  - Risks to national security, societal and public interests, or personal legitimate interests
Other International Developments – China

- Data Localization Requirement
- Data Subject Rights
  - Right of erasure
  - Right of data portability
  - Right to appeal automated decisions that directly impact the rights and interests

Key Takeaways for Employers

- Build Upon Your GDPR Compliance Program
- Provide Detailed Notice
- Accountability Documentation
- Compliance Documentation
- Breach Notification Readiness
- Upgrade Data Security Programs
- Self-regulation
- Vendor Management
- Leadership
Managing Employee Data Privacy:
A Worldwide Strategy for Multinational Employers

Presenters
Simon McMenemy (London) and Grant Petersen (Tampa)

Moderator
Bonnie Puckett (Atlanta)