IAPP Privacy Certification

Certified Information Privacy Professional (CIPP)

Workplace Privacy

James Koenig

Practice Co-leader, Privacy Strategy and Compliance

PRICEWATERHOUSECOOPERS

agenda

- HR privacy basics
- workforce hiring
- HR data management
- workplace monitoring
- employee misconduct
- termination issues

HR privacy basics

HR goals

- **Ensure that workplace risks are understood and managed appropriately**
  - Know your employees
  - Know what your employees are doing
  - Investigate potential issues
  - Avoid a “harassing” workplace
  - Meet training & compliance goals
  - Maintain necessary documents
- **Attract & retain excellent workers**
- **Provide excellent “customer service”**
- **Provide tools and data needed for corporate planning functions**
- **Manage costs associated with HR functions**

HR goals

To achieve these goals:

- Background checking new workers
- Monitoring worker activities to help ensure compliance with laws & policies
- Centralized HR databases
- Global intranet systems
- Connectivity technology, *e.g.,* email, online directories, instant messaging, remote access, portable memory devices
- Global benefits & compensation programs, advancement planning
- Use of data processing vendors & outsourcing for benefits, payroll, other functions

reality check

The business reality…

- All of these things are highly efficient, cost effective, and make perfect sense

The legal reality…

- HR data management requires careful consideration of liability issues…
  - In the US, for failing to process data
  - In Europe (& elsewhere) for processing data in violation of strict privacy laws
- Local laws in each country and state establish different requirements, with no harmonization in sight
- Civil and criminal penalties may apply

when issues arise

- **Before employment occurs:**
  - Application & interview questions 7
  - Testing
  - Background checks
- **During employment:**
  - HR data management
  - Workplace monitoring
  - Investigations of misconduct
- **After the employment relationship ends:**
  - Termination procedures
  - Transition management and ongoing obligations
  - Post-termination claims
  - Document retention and destruction

geography matters

- **This presentation focuses on U.S. privacy laws…**
  - **… but takes note of some significant points in non-US laws**
  - **Nations with comprehensive data protection laws and Works Council rules have very different regimes**
  - **Liability considerations make it difficult to offer US employees the kinds of privacy protections that counterparts elsewhere enjoy**

US-EU comparison

The Global Employer's Challenge

- **US gives rights to EMPLOYERS**
  - Security concerns predominate
  - Continuous and multi-dimensional employee monitoring okay
  - Aggressive background checks okay (& increasingly required)
  - Employee expectations of privacy are very limited
- **EU gives rights to EMPLOYEES**
  - Privacy concerns predominate
  - Monitoring only permitted with specific and limited legal justification
  - Limited background checks
  - Employees have broad privacy expectations and rights

world map

- **Europe: employee data covered by EU Directives, national data protection laws and distinct labor laws** 10
  - **Must comply with requirements for registration and processing – notice, choice, *etc.* – as well as restrictions on data transfers**
  - **Additional rules for "sensitive data"**
  - **Must consult with employee "works councils" on substantive matters**
  - **Even name and work address is protected**
- **Canada: EU-style law, but no protection for business contact data, limited protection for employee data, no special prohibition on export & no govt filings**
- **Japan: new EU-style law will cover all employee data effective 4-1-2005**

U.S. patchwork

- Many federal and state laws regulate employment and HR data management
- Federal laws seldom preempt stronger state protections
- Laws require and prohibit specific information handling practices at all stages of the employment relationship
- There is also a patchwork of regulators
  - *Department of Labor*
  - *Equal Employment Opportunity Commission – EEOC*
  - *Federal Trade Commission*
  - *State Departments of Labor*
  - *National and State Labor Relations Boards*

Almost every labor law mandates some data collection or management practice!

US federal laws

Laws that prohibit discrimination (& therefore limit inquiries)

- **Civil Rights Act of 1964** – no discrimination due to **race, color, religion, sex, national origin**
- **Pregnancy Discrimination Act** – added **pregnancy, childbirth, related medical conditions**
- **Americans with Disabilities Act** (ADA, 1990) – no discrimination against qualified individuals with **disabilities**
- **Age Discrimination Act of 1967**– protects individuals **over 40** years of age
- **Equal Pay Act of 1963** – prohibits **gender-**based wage discrimination
- Other laws regulate Federal and state government practices, including contractors

US federal laws

Laws that regulate employee benefits management – often mandate collection of medical information

- **Health Insurance Portability and Accountability Act (HIPAA) –**

  Privacy and Security rules regulate "protected health information" for self-funded health plans
- **Consolidated Omnibus Budget Reconciliation Act (COBRA) – requires qualified health plans to provide continue coverage after termination to certain beneficiaries**
- **Employee Retirement Income Security Act (ERISA) – ensures that employee benefits programs are created fairly and administered properly**
- **Family and Medical Leave Act (FMLA) – entitles certain employees to leave in the event of birth or illness of self or family member**

US federal laws

Other US federal laws with privacy implications – data collection and record-keeping requirements

- Fair Credit Reporting Act (FCRA) – regulates use of "consumer reports" in background checks of employees
- Fair Labor Standards Act (FLSA) – establishes minimum wage and sets standards for fair pay
- Occupational Safety & Health Act (OSHA) – regulates workplace safely
- Whistleblower Protection Act
- National Labor Relations Act (NLRA) – sets standards for collective bargaining
- Immigration Reform and Control Act – requires employment eligibility verification
- Federal employers also must consider Privacy Act of 1974 (requires privacy notices and limited collection of data) and the U.S. Constitution 4th Amendment ("search and seizure" limits)

state laws

- **State constitutional right of privacy**
  - **Apply to state government employees**
  - **Some states (*e.g.*, California) also apply it to private employers**
- **Specific state statutes (*e.g.*, no "marital status" discrimination, drug testing and polygraph laws)**
- **Common law torts:**
  - **Invasion of privacy (or "intrusion upon seclusion")**
  - **Defamation (*e.g.*, disclosure of info)**
  - **Intentional infliction of emotional distress**

hiring & re-employment inquiries

Pre-employment Inquiries

Name & Address

OK:

- Whether applicant has worked under a different name
- Name by which applicant is known to his references
- Requests for information needed to facilitate contacting the applicant

NOT OK:

- Inquiry into name before it was changed by court order or marriage
- Inquiry about a name that would divulge marital status, lineage, ancestry, national origin or descent
- Names or relationships of people with whom applicant resides
- Whether applicant owns or rents home

Pre-employment Inquiries

Age

OK:

- Inquiry as to date of birth
- Requirement of proof of age (especially when it relates to a job requirement)

NOT OK:

- Any questions that imply a preference for persons under 40 years of age

Pre-employment Inquiries

Height & Weight

OK:

- Employer may ask about height & weight only if employer can show that all or substantially all employees who fail to meet a height or weight requirement would be unable to perform the job with reasonable safety and efficiency

NOT OK:

- Any other questions about height or weight

Pre-employment Inquiries

Marital Status, Spouse,Relatives and Family

OK:

- Names of applicant's relatives already employed by the company or a competitor
- Whether applicant can meet certain work schedules or has activities, commitments or responsibilities that may prevent him/her from meeting work attendance requirements

NOT OK:

- Most other questions about spouses and relatives, including whether applicant even has or has had a spouse, children or other dependents

Pre-employment Inquiries

Pregnancy

OK:

- Questions about duration of stay on job or anticipated absences that are made to males and females alike

NOT OK:

- Questions about pregnancy or medical history concerning pregnancy and related matters

Pre-employment Inquiries

Disabilities

OK:

- Whether applicant is able to perform the essential functions of the job for which the applicant is applying, with or without reasonable accommodation

NOT OK:

- Questions about the nature, severity, extent of, or treatment of a disability or illness, including mental illness
- Inquiries (prior to job offer) about whether the applicant requires reasonable accommodation
- Whether applicant has applied for or received worker's compensation

Pre-employment Inquiries

Citizenship & National Identity

OK:

- Applicant's ability to read, write & speak foreign languages, where this relates to job requirements
- Whether applicant is prevented from lawfully being employed because of visa or immigration status
- Whether applicant can provide proof of a legal right to work in the country after being hired

NOT OK:

- Questions about national origin, lineage, ancestry, descent, birthplace, mother tongue of applicant or applicant's spouse or family
- Whether applicant is a citizen
- Requirement before job offer that applicant present birth certificate, naturalization, baptismal certificate

Pre-employment Inquiries

Military Service & Organizations

OK:

- Questions concerning education, training, or work experience in the armed forces of the U.S.
- Questions about organization memberships, except for organizations that indicate the race, color, creed, gender, marital status, religion, or national origin of members

NOT OK:

- Type or condition of military discharge
- Experience in armed forces other than U.S.
- Questions about organizations that indicate the race, color, creed, gender, marital status, religion, or national origin of members
- Requirement that applicant list all organizations to which he/she belongs

Pre-employment Inquiries

Gender, Race, Religion

NOT OK!

- Nothing on these topics is permitted…
- Includes questions concerning color of skin, hair, eyes
- Includes questions concerning church memberships and religious holidays observed

Pre-employment Inquiries

Photographs

NOT OK:

- **You cannot request applicants to submit a photo before hiring – even if the submission would be voluntary**
- **A photograph may be requested *after* hiring for identification purposes**
- **Posting of photos on public websites or even internal intranet sites should preferably be done with employee consent (especially in the EU where photos can be considered “personal data”)**

Pre-employment Inquiries

Arrests & Convictions

OK:

- Inquiries about convictions within the last 10 years for crimes involving behavior that would adversely affect job performance

NOT OK:

- Other inquiries about convictions
- Inquiries about arrests not followed by conviction (esp NY, CT, Wis)
- Some exemptions for orgs that provide care for vulnerable groups such as children, mentally ill, & for some other industries (such as financial services)

Pre-employment Inquiries

Alcohol & Drug Use

OK:

- Questions about current illegal use of drugs
- Questions about past illegal use of drugs, if not likely to elicit information about a disability, such as past addiction to illegal drugs
- Questions about alcohol use that are not likely to elicit information about alcoholism (a disability)

NOT OK:

- Questions about legal drug use
- Questions about past addiction to drugs (legal or illegal) or treatments for same
- Questions about alcoholism or treatments for same

Pre-employment Inquiries

References & Emergency Contact Information

OK:

- By whom were you referred for a position here?
- Names of persons willing to provide professional or character references
- Name and address of person to be notified in case of emergency

NOT OK:

- Questions about former employers or acquaintances which elicit information specifying the applicant's race, creed, color, national origin, ancestry, physical handicap, medical condition, marital status, age or sex
- Questions about relationship of the emergency contact to the applicant
- May not require the contact to be a relative

applicant testing

applicant testing

Types of testing employers use:

- Personality & Psychological Testing
- Polygraph (“Lie Detector”) Tests
- Substance Abuse (“Drug”) Tests
- Genetic Tests

personality & psychological tests

- **Personality & Psychological testing includes:**
  - Cognitive ability tests
  - Honesty & Integrity tests
  - Interest inventories
- **Types of tests:**
  - "Performance" aka "Situational" Test taker is asked to react to a real-life situation and is assessed in response.
  - "Projective" (ask test taker to interpret ambiguous stimuli and respond in an open-ended manner) (*e.g.*, Rorschach)
  - "Objective" (true/false & multiple choice)

psychological test risks

- **Tests may be construed as a "medical examination" under the ADA**
  - Projective and Objective tests are especially risky because they were originally developed to identify clinical conditions such as depression, paranoia
- **State law tort claims may include:**
  - Violation of anti-testing laws
  - Invasion of privacy or intrusion upon seclusion
- **And for publicizing or leaking test results:**
  - Public exposure of private facts
  - Publicity placing a person in false light
  - Defamation
  - Intentional infliction of emotional distress

mitigating the risks of tests

- Don't use the tests at all – or else don't use the tests pre-employment
- If used, ensure that test:
  - Asks only job-related questions
  - Does not ask overly-intrusive questions
  - Is professionally designed with established reliability and validity
  - Is administered & interpreted by trained professionals
  - results are limited to those with a need to know & used only for the purposes for which test was designed & validated
- Best practice: obtain employee's consent to test and to the specific uses of the results prior to administering test (required in EU)
- Also consider collective bargaining issues (Unions on US & Works Councils in EU)

lie detector tests

Employee Polygraph Protection Act of 1988

- "Lie detector" includes polygraphs, other devices which render a diagnostic opinion on a person's honesty
- The Act generally prohibits employers:
  - requiring, requesting or even suggesting that a prospective or current employee take a lie detector test
  - using, accepting, referring to or inquiring about test results
  - taking adverse action against employee who refuses a test
- Narrow exemptions for investigations of economic loss or injury, certain industries
- Requires posting the Act's essential provisions in a conspicuous place
- Possible $10,000 fine; private right of action
- State laws not pre-empted; torts may apply

drug tests

No drug testing program is immune from legal attack!

- **Types of substance abuse testing:**
  - Pre-employment screening
  - Routine testing
  - Reasonable suspicion testing
  - Post-accident testing
  - Random testing
  - Rehabilitation/post-rehabilitation tests
- **Pre-employment screening**
  - Generally allowed in US if not designed to identify legal use of drugs or past or present addiction to illegal drugs (ADA)
- **Routine testing**
  - Generally allowed in US if employees notified at hiring

drug tests

- **Reasonable suspicion testing** 37
  - Generally okay in US to test as a condition of continued employment if there is a "reasonable suspicion" of drug or alcohol use based upon specific, objective facts and rational inferences from those facts (*e.g.*, appearance, behavior, speech, body odors)
  - Need not be "probable cause"
- **Post-accident testing**
  - Generally okay in US to test as a condition of continued employment if there is a "reasonable suspicion" that the employee involved in the accident was under the influence of drugs or alcohol

random drug tests

- Legality questionable in US except where required by law, prohibited in some jurisdictions (*e.g.*, Ontario)
- Example: random drug testing program required in US by DOT for commercial vehicle operators, but prohibited in Ontario unless employees consent to it.
- US cases upholding testing usually involve existing employees in specific, narrowly defined jobs that are either:
  - part of a highly-regulated industry where the employee has a severely diminished expectation of privacy, or
  - critical to public safety or the protection of life, property, or national security
- If used, random testing should be part of a systematic testing program that does not target certain employees or classes

drug tests

Rehabilitation and Post-rehabilitation Tests

- Commonly used a condition of continued employment during or after rehabilitation of an individual for substance abuse
- Generally allowable in the US
- To minimize risk for company, make the terms clear to the employee – company and employee should enter into contract addressing the terms of the rehabilitation and testing

alcohol tests

- Tests for alcohol levels generally are subject to the same rules as drug tests
- Tests for blood alcohol levels are better indicators of current impairment than tests for drugs, because traces of drugs stay in the body much longer after usage
- Less invasive tests more likely to be approved (*e.g.*, breathalyzer v blood sample).

genetic testing

- **"Genetic Screening"** involves examining the genetic makeup of employees or job applicants for certain inherited characteristics
  - Screening for trait that makes employee susceptible to pathological effect if exposed to certain agents
  - Screening to detect general inheritable conditions
- **"Genetic Monitoring"** involves periodic testing to identify modifications of genetic material, such as chromosome damage, that may have resulted from workplace hazardous materials

genetic testing

- **Criticisms of Genetic Testing:**
  - May be used to screen out individuals who are at higher risk of "disabilities" under ADA
  - May be used to screen out individuals who are at higher risk of developing non-occupational conditions that impact group insurance rates
- **Potential Legal attacks:**
  - ADA
  - Specific state "anti-testing" laws
  - Common law tort claims
- **Employer best practices:**
  - Test only where really related to job performance or to benefit the employee (*e.g.*, detect damage due to hazards)
  - Obtain specific consent for the test, not just consent to general medical exam

background checks

background checks

- Many laws mandating background checks among employees and applicants were enacted by US states in 2003 44
  - 165 statutes in 39 US states mandate some form of employment-related background investigations
- Heightened concerns about security and publicized instances of employee misconduct are driving these laws
- Some states also recognize tort of "negligent hiring," where employer is liable for damages caused by employee when it should have known of employee's propensity to commit injury

background checks

Groups targeted in background check laws:

- Teachers and other school employees
- Health and long term care facilities
- Emergency medical service personnel
- Programs for the disabled
- Financial institution personnel
- People providing money transmission and currency exchange services
- County coroners
- Humane society investigators
- Euthanasia technicians in animal shelters
- Bus drivers, truck drivers
- Athletic trainers
- In-home repair services (e.g., plumbers)
- Firefighters
- Gaming industry employees
- Real estate brokers
- Information technology workers (in ND)

background checks

Elements of Employee Background Checks:

- Criminal records
- Civil litigation history
- References -- professional, and sometimes personal as well
- Motor vehicle records (driving history)
- Credit records
- Licensure (if applicable)
- Professional Credentials
- Education (school transcripts)

background checks

Remember the restrictions on questions you can ask during the hiring process! Background check before job offer should *not* include any inquiries into:

- **Arrest record (but may research convictions within the last 10 years for a crime involving behavior that would adversely affect job performance)**
- **Age, Race, Religion, National Origin**
- **Health/Disability/Pregnancy (except for ability to perform functions of job)**
- **Financial status (unless specifically relevant to the position)**
- **Military status (*e.g.*, type of discharge rather than training)**
- **Family status (*e.g.*, whether applicant has a spouse, children or dependents)**

background checks

Fair Credit Reporting Act (FCRA)

- **Fair Credit Reporting Act (FCRA) applies when employer obtains a "consumer report" from a "consumer reporting agency" (CRA)**
  - "Consumer reports" include all written, oral or other communications bearing on a consumer's credit-worthiness, credit standing and capacity, character, general reputation, personal characteristics, or mode of living
  - "Consumer reporting agency" includes any organization that assembles or evaluates consumer credit information for the purpose of regular furnishing of consumer reports to third parties for a fee
- **Examples:**
  - Credit report obtained from credit bureau
  - Driving history report obtained from information aggregator

background checks

Fair Credit Reporting Act (FCRA)

- **FCRA prohibits obtaining a "consumer report" unless a "permissible purpose" exists**
- **Employers have a permissible purpose to use consumer reports for:**
  - **Pre-employment screening**
  - **Determining if an existing employee qualifies for promotion or advancement**

  But only with the person's written consent
- **FCRA also permits obtaining an "investigative consumer report" – a consumer report containing information that came from interviews with third parties, such as neighbors and friends of applicant – as long as certain additional protections are met**

background checks

Fair Credit Reporting Act (FCRA)

In order to use 3rd party data for FCRA purposes, the employer must:

- **Provide written notice to the applicant that it is obtaining a consumer report for employment purposes**
- **Obtain written consent from the applicant**
- **Obtain data from a CRA – an entity that has taken steps to assure the accuracy and currency of the data**
- **Certify to the CRA it has a permissible purpose and has obtained consent**
- **BEFORE taking an adverse action (such as denial of employment), provide notice to the applicant with a copy of CR**
- **AFTER taking an adverse action, provide additional notice**
- **Civil & criminal penalties for non-compliance**

background checks

- **Bankruptcy records:**
  - US Bankruptcy Code 11 USC 525 prohibits certain forms of employment discrimination against persons who have filed for bankruptcy, but courts are split on whether this applies to a hiring decisions before an offer is extended & accepted.
- **Driving Records:**
  - Available from state departments of motor vehicles. Subject to state "Driver's Privacy Protection Acts" but generally obtainable for employment screening in accordance with FCRA
- **Academic Records**
  - Confidential under Family Educational Privacy Rights Act (20 USC 1232g); most schools will not release without student's consent

HR data management

managing HR data

HR data management encompasses many different considerations:

- Legal compliance with the multitude of laws that regulate employee data and the employment relationship generally
- Security -- the protection of HR data from unauthorized use and authorized misuse
- Risk management – ensuring that proper documentation exists to manage any potential claims against the company (as well as claims the company may have against its employees!)
- Compliance with other corporate policies – substantive training, workplace liability management, document retention, *etc.*

getting classy

- **Data elements should be classified based on:**
  - Sensitivity (*e.g.,* SSN, medical data)
  - Country of origin
  - Other legal restrictions (*e.g.,* data collected for EEOC compliance)
- **Company employees and managers should also be classified – permit access to HR data based on roles**
  - Company directory may available to all, but SSN on a need-to-know basis
  - Special controls on data related to performance reviews, workplace investigations

things to know

- **Understand your data flows**
  - Where is data is collected?
  - What data is collected?
  - How is it stored?
  - How is it secured?
  - Who has access internally?
  - What third parties have access & why?
  - When and how is it destroyed?
- **Understand your vendors as well**
  - Service providers (*e.g.*, benefits)
  - Outsourcers (*e.g.*, payroll processing)
  - IT and other corporate suppliers
- **Vendors should have role-based access as well**

security issues

HR functions handle some of the most sensitive data in the company – must have a written program that encompasses:

- **Administrative Security**
  - Program definition & administration
  - Managing workforce risks
  - Employee training
- **Technical Security**
  - Computer systems, networks, applications
  - Access Controls
  - Encryption
- **Physical Security**
  - Facilities
  - Environments safeguards
  - Disaster recovery

vendors

- Outsourcing is a key economic driver, whether on-shore or off-shore – and HR data processing is one of the most frequently outsourced functions
- US privacy laws generally anticipate use of vendors and service providers and do not restrict transfers of data based on geography – but recent anti-outsourcing bills are attempting to limit outsourcing and require more disclosures about it
- Companies always remain accountable for actions by their agents – so security is the biggest consideration

Best practices:

- Establish a formal vendor security qualification protocol and audit against it
- Have established vendor contract provisions:
  - Limiting scope of use of data
  - Mandating reasonable security
  - Mandating confidentiality
  - Mandating notice of any security or confidentiality breach
  - Providing for audit rights, insurance, indemnification

if there's an 'oops

- If you have a security breach involving certain types of unencrypted sensitive personal information (e.g., SSNs or account numbers), California law requires you to promptly notify any affected California residents
- If individuals may be harmed as a result of a security breach, you should notify them even if they aren't California residents. This is not required by a statute, but may help avoid tort liability if they become victims of ID theft
- HR databases are prime targets for ID thieves because of the presence of SSN and date of birth

other laws

Don't forget your collective bargaining agreements either!

Don't forget that other laws may regulate your HR processing. For example:

- EU, Canadian and other non-U.S. data protection laws, if you have workers outside the U.S.
- U.S. State and federal laws that require collection of data (such as race for EEOC reporting)
- Laws that require reporting of events that affect health & safety (*e.g.,* OSHA)
- HIPAA regulates employer-sponsored health plans (but does *not* cover other medical data that may exist in the workplace)
- Some state laws require privacy notices before monitoring or surveilling

employee monitoring

why monitor

- **Risk management**
  - Prevent "hostile environment" claims
  - Prevent workplace violence
  - Prevent theft, loss of intellectual property
- **Quality control**
- **Productivity metrics**
- **Public health & safety – may be required by laws**
- **Corporate compliance (*e.g.*, document retention)**
- **May also use monitoring data for secondary purposes**
  - Investigation of misconduct or loss
  - Performance reviews

how to monitor

- Workplace surveillance (*e.g.*, CCTV)
- Employee sign-in, log-in records
- Access controls
  - Badge cards & readers
  - Biometric access controls
- Automated online monitoring
  - Virus filters
  - Spam filters
  - Logging website URLs
  - Spidering hard drives for file titles
- Specific monitoring
  - Telephone
  - Computer
    - E-mail
    - Internet Access

issues

- Situations when you *must* monitor
- Restrictions on monitoring
  - Private spaces
  - Employee notices and consents
- Secondary use of monitoring data (*e.g.*, performance reviews)
- "*Ad hoc*" monitoring – for a particular purpose, but outside of established protocols
- Liability issues

audio & video

- State and federal wiretap laws
  - Must get consent of at least one party – and all parties must consent in 12 states
  - Recorded "call may be monitored" message to all parties will be adequate notice in most jurisdictions
  - Be careful of *ad hoc* monitoring
  - General rule – cannot listen to employee personal conversations; must discontinue monitoring as soon as it is apparent that the call is personal
- Video monitoring is less regulated (as long as the sound is off)
  - Very little expectation of privacy in the workplace in US, especially if notice given
  - But cannot monitor in truly private spaces (*e.g.*, restrooms, locker areas)

computers

- Electronic spaces are even less protected than physical spaces in the U.S.
- Computer systems belong to the employer and US employees generally have no expectation of privacy in use of employer equipment
  - Electronic Communications Privacy Act (ECPA) prohibits intercepting electronic communications and unauthorized access to stored communications, but includes
    - "business use" exception
    - "employee consent" exception
- But some states do require notice:
  - Delaware requires advance and acknowledged notice to employee of monitoring of telephone, electronic mail and internet

EU and other places

- **More restrictive policies in the EU:**
  - **Monitoring must "proportionate" to the practices that it is intended to detect or prevent**
  - **Monitoring practices must be specifically disclosed to employees and to Works Councils**
  - **Some monitoring may require consent**
  - **Disciplinary action for monitored behavior may be limited under EU labor laws**
  - **All data transfer and other rules apply to monitoring information as well**
- **Other jurisdictions with strict rules include Canada, Argentina, Japan**

managing the issues

- **Establish formal policies for monitoring**
  - When you will monitor
  - When you can monitor
  - How data will be used
  - What happens when you find something serious
  - Ensure compliance with applicable laws and collective bargaining agreements
- **Provide employees with notices regarding monitoring and related considerations**
  - Ownership of company computers
  - Prohibited conduct
- **Have process ready to handle exceptions and special circumstances**

investigating employee misconduct

employee misconduct

Allegations of misconduct raise special concerns

- Liability (or loss) for failure to take allegations seriously
- Reasonably protecting the employee during the process – *due process*
- Ensuring compliance with other corporate polices
- Ensuring compliance with external obligations (laws, collective bargaining agreements)
- Documenting the misconduct and otherwise minimizing likelihood of successful employee claims
- Balancing the rights of other people who may be involved (such as person making the allegations)

third party help

- Companies often rely on third-party investigators to conduct investigations of wrong-doing properly
- In 1999, the Federal Trade Commission ruled that reports from third-party investigators should be considered “investigative consumer reports” subject to all FCRA provisions:
  - Obtain consent beforehand
  - Notify with copy of report prior to adverse decision
  - Adverse action notice
- This ruling hampered corporate efforts to manage investigations

third party help

- **The 2003 amendments to the FCRA exclude investigation reports from coverage *if:***
  - **The report is prepared as a result of an investigation of specific "suspected misconduct related to employment" or compliance with laws, regulations or pre-existing policies of the employer**
  - **The report does not include an investigation of credit worthiness, standing or capacity**
  - **The report is only given to the employer, its agents, government regulators and self-regulatory organizations**
- **But if an adverse action is taken, a summary of the report must be provided with an FCRA adverse action notice**

termination of the employee relationship

when it's over

Privacy considerations exist at the end of the employment relationship:

- **Document reason for termination – classify as sensitive data**
- **Curtail employee access to company information – disable computer accounts, repossess access devices**
- **Seek return of personal data that employee may have had (*e.g.*, company directories, computer storage devices)**
- **Remind individual of obligation to maintain confidentiality of employer data (if applicable)**

what to say

- **Carefully craft messages regarding termination – especially if relationship terminated as a a result of misconduct**
  - **Internal messages to remaining employees – especially if you want to "make an example" of the individual**
  - **Messages to customers**
  - **Messages to companies seeking future references**
  - **Messages to regulatory agencies, if applicable**
- **Providing references**
  - **Consider privacy interests**
  - **Understand applicable defamation risks**
  - **But consider honesty, especially if health or safety is at risk**

what to store

- Consider what documents to retain in HR files – where and for how long
- Company document retention policy should control – if policy doesn't exist, develop formal HR data retention policy based on:
  - Ongoing obligations (pensions, COBRA, *etc.*) and company re-hire policy
  - State and federal retention requirements
  - Applicable statute of limitations
  - Corporate risk tolerance
- Ensure secure storage with proper access controls
- When documents are no longer needed, ensure secure disposal (*e.g.*, shredding)

final thoughts

Thoughtful management of employee personal information can help reduce the risk of claims… but other benefits exist too

- **Reduce risk of ID theft affecting employees – good for them and reduces productivity loss as well**
- **Improved employee moral**
- **Equity for use in collective bargaining**
- **Sensitivity to employee concerns bolsters company claims of sensitivity to consumer privacy**
- **In the event of a claim, you've got a good story to tell – which may reduce the risk of damages**
- ***It's also the right thing to do!***

IAPP Certification Promoting Privacy