SQUIRE SANDERS

Top Data Protection Worries for HR Professionals in Europe and the US

Ann J. LaFrance
Philip R. Zender
Karin Konstantinovova

Selected U.S. Law Considerations

- No one law governing employment and workplace privacy; instead, complex patchwork of multiple federal and state laws and regulations covering privacy-related issues in both the private and public sector.
- These multiple laws and regulations cover 3 separate phases:
  - (i) before hiring phase when candidates are being considered for employment;
  - (ii) during the actual employment phase; and
  - (iii) post-employment phases after the employment relationship has terminated.
- Today's presentation on U.S. legal issues will focus on:
  - **Use of social media to screen and monitor** (before and during employment);
  - **Monitoring in the workplace** (during employment); and
  - **BYOD (or "bring-your-own-device")** (during and to some extent after employment).

Social Media-Related Privacy

- Screening: Use of social media to screen prospective employees has become common.
  - There is no legal prohibition against tracking individuals online and screening candidates for certain factors selected by employer, such as drug use or unsafe behavior.
  - However, such screening must be done in a manner that is not and does not appear discriminatory (e.g., avoid focusing on information that pertains to protected classes, such as religion, ethnicity, gender and sexual orientation).
    - This may require specific training and internal policies.
- Monitoring: Social media monitoring may also be used to keep track of current employees in connection with brand reputation concerns.
- Seeking Access to Private Accounts: Employers should avoid the use of deceit or manipulation to gain access to private information:
  - Communicating with prospective employees through false online profiles.
  - This may be considered a violation of a person's reasonable expectation of privacy and be actionable in tort.

Social Media-Related Privacy

REQUIRING ACCESS TO PRIVATE ACCOUNTS

- Employers should not require prospective or current employees to provide access information to private networks as a condition of employment, such as social media usernames and passwords.
- This is prohibited by the laws of various states.
  - Rationale: employers generally do not have access to employee's personal email account and social network accounts should not be treated differently.
- In 2012 CA passed legislation (A.B. 1844) that prohibits an employer from requiring or requesting an employee or applicant for employment to (i) disclose a user name or password for the purpose of accessing personal social media, (ii) to access personal social media in the presence of the employer, or (iii) to divulge any personal social media.
  - Prohibits an employer from discharging, disciplining, threatening to discharge or discipline, or otherwise retaliating against an employee or applicant for not complying with a request or demand by a violating employer.
  - A pending bill would apply these provisions to public employers within CA at both a state and local level.

Monitoring in the Workplace

- There are good reasons for monitoring employees in the workplace:
  - promoting workplace safety, protecting physical security and trade secrets, improving work quality and keeping employees focused on work tasks.
  - Federal Occupational Safety and Health Act of 1970 requires employers to meet certain safety standards and to ensure that employees are performing tasks in a safe manner. Compliance with OSHA may justify monitoring.
- Generally, employers in private sector have broad authority to do monitoring and searches at work; therefore, private-sector employees have limited expectations of privacy at the workplace.
  - E.g., Computers and IT equipment are usually the property of the employer who may, therefore, control the use of such equipment.
- Nonetheless, employers should establish formal policies about workplace monitoring and related documents, such as acceptable use policies for IT equipment.
  - These are generally effective in addressing employee tort-based privacy invasion claims re monitoring, which might otherwise be available to employees.
  - However, once these policies are established the employer should not exceed their limitations.

Monitoring in the Workplace

- Video Surveillance: Camera and video recordings without sound fall outside the scope of the federal wiretap laws and are not prohibited by federal law. Therefore, it is generally permitted to use closed circuit television and other video surveillance in the workplace to promote safety and avoid theft by third parties or employees.
  - However, state laws create certain limits – e.g., invasion of privacy tort and CA and other state statutes prohibit videos recordings in areas such as restrooms and locker rooms. Such recordings may also be actionable under a common-law tort claim for invasion of privacy, or prohibited by collective bargaining agreements.

- Intercepting Communications: The Electronic Communications Privacy Act (ECPA) applies to government and law enforcement officials AND private parties and is therefore applicable in the private sector workplace.
  - ECPA generally prohibits interception of wire communications (e.g. telephone calls), oral communications (e.g. hidden microphones) and electronic communications, such as emails.
    - Unless an exception applies, such interceptions are a criminal offence and ECPA provides a private right of action.

Monitoring in the Workplace

- Two exceptions apply in the workplace:
  - One party to a communication has consented to the interception or access; and
  - The interception is done in the ordinary course of business (e.g. routine monitoring in a call center)
    - However, as courts have split on how broadly to define the "ordinary course of business," it may be best to rely on consent, which should be express. But:
      - employers must act within the confines of such consent, which may preclude monitoring personal communications; and
      - The ECPA does not preempt state laws and some states require consent from both parties to the communication (the reason customers often hear a message giving notice that a call is being monitored for quality control purposes).
- Compliance:
  - Notify employees of monitoring policy- this will establish consent
  - Acknowledgement in writing is best

Monitoring in the Workplace

- Postal Mail Monitoring: Federal law prohibits interference with mail delivery. But mail is deemed "delivered" when it reaches the business address.
  - Therefore, an employer representative may open letters and packages even if he is not the intended recipient without violating the law.
  - However, to avoid risks under state common law, if practical, employers should advise employees not to have personal mail sent to work, and should avoid reading personal letters and keep any personal information inadvertently obtained confidential.
- Location Monitoring: Employers may use mobile phones and GPS devices to monitor the location of company vehicles.
  - But such monitoring should be for business purposes during business hours and employees should be informed in advance.
  - Monitoring the location of employees should generally be avoided.
    - It raises the risk of invasion of privacy tort claims in situations where the employee has a reasonable expectation of privacy.
    - Also, CA criminal law prohibits the use of an electronic tracking device to determine the location or movement of state employees.

BYOD Generally

- The availability and general "consumerization of information technology" (aka COIT) has led to an increase in the number of individuals using their personal devices (e.g. laptops and mobile phones) for work purposes – a trend referred to as "bring your own device" (or BYOD).
  - Studies estimate that approximately 45% of U.S. employees are using personal devices for work purposes.
  - Advantages:
    - greater flexibility and convenience for employees and reduced expenses for employer;
    - may make employees more productive; and
    - fosters an image of flexibility on the part of the employer.
      - Reality - virtually inevitable that employees will use their own devices for work.
- BYOD Policies
  - Important to have written policy that outlines
    - The responsiblities of the user; and
    - The employer's rights with respect to BYOD technology
      - E.g., use of mobile device management (MDM) software to manage device.

BYOD Security Concerns

- BYOD has security implications may present significant security challenges and risks to employer and company data due to lack of control over devices.
  - May increase risk of data breaches (e.g. if employee loses smartphone on weekend outing that she uses to access the company network).
  - Employee storage of data in the Cloud.
  - Sharing of devices with others (e.g., family members).
  - Need to align employer security policies with employees' use of devices for work purposes. Generally, the same security controls used for employer issued devices should be used on private devices – e.g. use of passwords, installation of firm supplied encryption applications for use on data transferred between personal device and employer, use of technology that enables employer to remotely delete data in the event of loss of the device.
  - Use of MDM software can address some of these security concerns.
  - Need to ensure that use of personal device and security controls required for such devices are generally consistent with employer's statements in privacy policies and other security-related legal requirements.

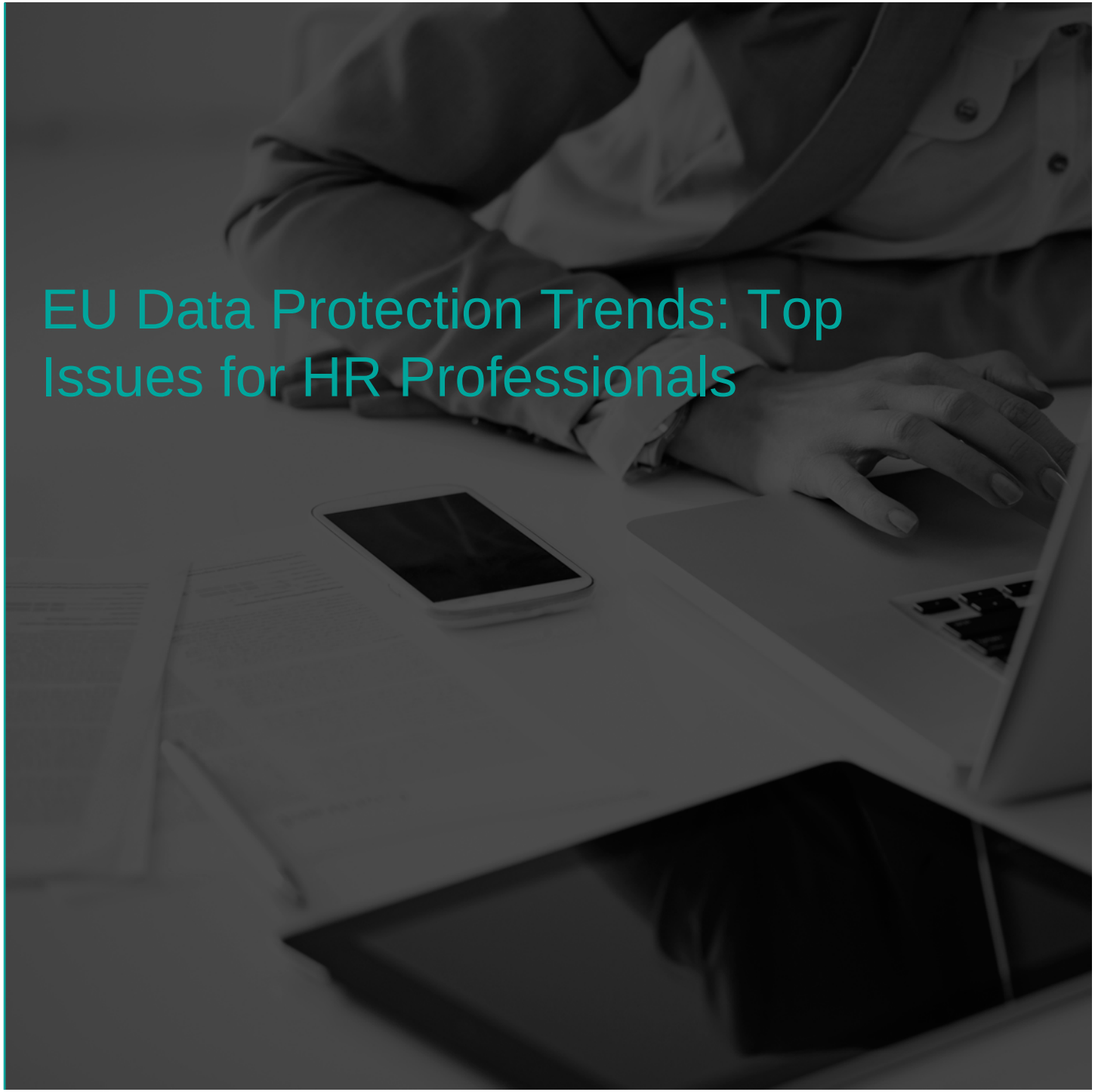
BYOD Policies and Procedures

Generally, when designing and implementing BYOD policies and procedures, the following factors should be considered:

- Define what sensitive company information needs to be protected, which employees should have access to such information via their personal devices
- Require device be given to employer:
  - Before activation so that security protocols (e.g. encryption) and software (e.g. MDM software) may be installed
  - Upon termination to permit removal of sensitive information
- Define what sensitive company information needs to be protected, which employees should have access to such information via their personal devices
- Require the use of robust passwords that must be changed periodically
  - This requirement can be pushed to the device using MDM software
- Inform employees of privacy limitations that will result from using their own devices in the workplace
- Require immediate notification of lost or stolen devices
- Wiping of data – note that the device may be remotely wiped by the employer and that personal data (e.g. pictures, notes, emails, etc.) may be lost unless backed up
- Consider and address the status of phone numbers upon termination of employment
- Obtain express written consent to any device monitoring or surveillance and the BYOD program generally (to avoid problems of unauthorized access under ECPA, SCA, CFAA and similar laws)
- Provide for appropriate training on the policy

SQUIRE SANDERS

EU Data Protection Trends: Top Issues for HR Professionals



Agenda

1. Data Breach Response
2. Bring Your Own Device (BYOD)
3. Safe Harbor and International Data Transfers / Cloud
4. HRIS Platforms
5. Whistleblower Hotlines
6. Employee Monitoring and Cross-Border Investigations
7. Data Subject Access Requests
8. Proposed EU Data Protection Regulation
9. Closing thoughts

1. Data Breach Response

ISSUE:

EU DP Rules impose specific requirements for storing, processing and transferring personal data about EU employees -- employer's liability exposure is increased by failure to prepare for data breach incidents.

Action Steps:

→Prepare

- **Do you have an inventory of HR personal data that is stored and processed in the EU?**
- **Is EU HR data shared or potentially shared with points outside the EU and processed or stored there?**
- **Have you identified risks and vulnerabilities?**
- **Do you work with cloud providers? Where do they keep the data and is it secure?**
- **Do you have a Data Breach Response Plan in place?**
- **Does your company's insurance cover cyber risk?**

1. Data Breach Response (cont'd)

→ **Prevent**

- **Are your operations as secure as they can be/need to be (physical, technical organizational safeguards)?**
- **How are you protecting the data of your mobile workforce?**
- **Have you properly vetted the security measures implemented by any cloud providers/other contractors that are involved?**
- **Has your company carried out a security audit of IT systems that process/store HR personal data?**
- **Do you have the right to audit third-party vendors?**
- **Do you have written contracts with your contractors that fully address use and protection of personal data**

1. Data Breach Response (cont'd)

→ Detect and Respond

- **Are employees up and down the line aware of your Data Breach Response Plan?**
- **Have you identified a Crisis Response Team (internal and external) for dealing with data breaches, and are employees aware of who they are?**
- **Are you prepared to deal with the consequences of a serious data breach?**
  - Technical
  - Commercial
  - Legal
  - PR

1. Data Breach Response (cont'd)

→ **Recover**

- **Is your data sufficiently backed up and can it be restored?**
- **Do you have feedback loops in place to identify any changes required to address lessons learned?**

2. Bring Your Own Device (BYOD)

ISSUE:

EU DP Rules impose obligations on data controllers (employers) to ensure the security of personal data they hold about their employees.

- ***User devices can easily pass malware and viruses onto company platforms and impact security levels.***
- ***Co-mingling personal data of employees with company data may complicate compliance with EU data protection rules.***

Things to Consider:

- Have you assessed the legal and regulatory implications and risks of allowing employees to use their own devices and associated cloud suppliers?
- Do you have an effective and well-publicized BYOD program in place?

3. Safe Harbor and International Data Transfers/Cloud

ISSUES:

→ *The Snowden revelations have called into question many assumptions underlying the US-EU Safe Harbor Program.*

- *The European Commission has made 13 Recommendations to restore the trust in data flows between the US and the EU and will decide on the future of the existing framework this summer.*

→ *EU data protection regulators are increasingly concerned about the security of third-party cloud services, especially those involving shared servers.*

- *The EU Commission and some Member State DP Authorities are issuing guidance on "safe and fair" contract terms and conditions for cloud computing services.*
- *A "European Seal" program is under consideration to identify EU DP-compliant cloud providers.*

3. Safe Harbor and International Data Transfers/Cloud (cont'd)

Things to Consider:

- If your company is Safe Harbored, have you developed contingency plans to deal with expected changes/potential discontinuance?
- Are you aware of the EU-approved alternatives to Safe Harbor?
- Do your contracts with cloud providers require them to take the same security measures as your company would implement in-house?
  - Do the terms comply with EU DP Rules?
  - What obligations does your cloud provider have in case of a data breach?
  - Are there any indemnities, limitations or exclusions in relation to data breach?

4. HRIS Platforms

ISSUE:

Employers must abide by EU data protection rules when rolling out a global HR information system involving the processing of EU employee data outside of Europe.

Things to Consider:

- Do you know which personnel have access to EU employee data outside of Europe, and for what purpose?
- Have you legitimised transfers outside the EU via the use of Safe Harbor, the EU Standard Clauses and/or Binding Corporate Rules?
- Have you provided EU employees with adequate notice, consulted or signed agreements with employee representatives (of any works council) and updated DPA registrations where required?
- Are cloud providers involved and are transfers to them compliant with EU law?

5. Whistleblower Hotlines

ISSUE:

U.S. law requires publicly traded companies to establish anonymous whistleblower hotlines; however, anonymous "snitching" is not acceptable in some EU Member States, which apply varying rules and approval procedures to global whistleblower hotline schemes.

Things to Consider:

- Are you aware of the cultural sensitivities and hotline limitations in the different EU Member States where your company operates?
- Does your hotline solution adhere to local rules to the extent possible?
- Do you keep up-to-date with changes in these rules? For example:

5. Whistleblower Hotlines (cont'd)

UPDATE - FRANCE

- In January 2014, the French DP Authority issued a decision that widens the scope of permissible reporting under a whistleblower hotline scheme.
- Previously, reporting was only justified to disclose a breach of legal requirements under French law in limited areas: finance, accounting, banking, anti-corruption and antitrust, as well as under the Sarbanes-Oxley Act and its Japanese equivalent.
- Reporting is now also allowed if it is in the "legitimate interests" of the company in the fields of: (1) harassment; (2) discrimination; (3) health, hygiene and security in the workplace; (4) protection of the environment; and (5) antitrust law.

UPDATE – HUNGARY

- A new law enacted in January 2014 imposes a number of new obligations on whistleblower hotlines.
- This includes an obligation to register the hotline with the Hungarian DP Authority.

6. Employee Monitoring and Cross-Border Investigations

ISSUE:

EU rules limit the ability of EU legal entities to process personal data within Europe, and to transfer it to foreign affiliates and third parties, including non-EU governmental authorities.

Things to Consider:

- Does your company have internal policies in place covering email and internet use/monitoring; information security; CCTV and telephone monitoring?
- Are you aware of the issues raised by a U.S. parent company's request for access to emails and/or web logs of EU employees?
- Conflict of laws: How to comply with requests for access to EU personal data (e.g. company emails) by foreign government authorities, litigants, etc. without violating EU DP Rules?

7. Data Subject Access Requests (DSARs)

ISSUE:

EU data protection rules give employees the right to access personal data about them that is held by their employer, and also to correct inaccurate information or request its deletion.

Things to Consider:

- Do your EU affiliates have Data Protection Compliance Officers in place or a clearly identified individual responsible for dealing with DSARs?
- Is management generally aware of the relevant local rules relating to DSARs?
- Does your company have procedures in place to deal with situations in which an employee seeking access to their file is also involved in an employment dispute?

8. Proposed EU Data Protection Regulation

ISSUE:

A new and highly controversial Regulation on data protection is currently being debated by the EU institutions and, if adopted, will become directly enforceable law in all EU Member States.

HIGHLIGHTS

- Regulation (versus "Directive") should harmonise DP Rules across Europe, but enhanced protections are likely to apply.
- The Regulation will apply extraterritorially and will catch legal entities with no physical presence in the EU if they process personal data in connection with the monitoring of EU residents.
- Sanctions for non-compliance with the Regulation include maximum fines of EUR 100 Million or 5% of global turnover (whichever is higher) for serious breaches.

8. Proposed EU Data Protection Regulation (cont'd)

- Private right of action for victims – non-pecuniary damages covered.
- Employers will be required to notify local data protection authorities and victims of a data breach "without undue delay" [Note: apart from Germany, current rules on data breach notification only apply to telecoms companies].
- Employers must seek authorisation from local data protection authorities prior to any disclosure of EU personal data to a non-EU government or court (e.g., under Patriot Act); data subjects must also be informed.
- Employers will be required to appoint a Data Protection Officer where data processing relates to sensitive data (for example, criminal records checks, medical records etc.) [Note: DPOs are already required in some Member States, e.g. Germany, Slovakia]
- Employers will be required to forward any requests for deletion of personal data on to third parties (e.g. cloud providers, recruitment/vetting agencies, benefits providers and payroll providers).

9. Closing Thoughts

1. **It is difficult to be 100% compliant with EU DP Rules, but clear evidence of good faith efforts to meet core requirements will limit an employer's regulatory exposure.**
2. **The potential cost/risk of non-compliance is increasing (penalties and potential damages).**
3. **Works councils are keeping a close eye on employer compliance steps.**
4. **The EU has signalled that many of the specific "enhanced requirements" contained in the Draft Regulation are already required under the current DP Directive.**
5. **Safe Harbor is likely to survive, but with increased obligations on the part of U.S. "data importers" and stepped-up enforcement by U.S. regulators.**
6. **Forward planning will pay dividends in our data-driven economy.**

SQUIRE SANDERS

Czech Republic

Security measures and Project

- The personal data controller is obligated to adopt such measures, which are necessary for protection of the personal data against
  - unauthorized or incidental access, change, destruction or loss
  - unauthorized transfer
  - other unauthorized processing
  - other misuse of the personal data
- The adoption of such measures must be documented in a security project, including the following:
  - scope of persons authorized to access the personal data and the scope of their authorization with respect to the personal data
  - detailed description of measures preventing unauthorized access or other unauthorized processing of the personal data technical measures adopted in order to fulfill the obligation to evidence access to the personal data;
  - measures adopted to protect data storage media and prevent unauthorized access to such storage media

Evidence of access, consent of data subject

- The personal data controller is obligated to keep evidence of persons, who have accessed the personal data included in any of its automated system, including the following information:
  - who has accessed the personal data
  - when was the personal data accessed;
  - purpose of the accessing of the personal data; and
  - steps taken by such access
- Consent of data subject
  - Personal data may be processed based on:
    - Provision of law (i.e. without consent of the data subject), or
    - Consent of the data subject
  - Processing on the basis of law is usually limited
  - For effective HR management, consent of the employee with data processing is required, as it covers wider scope of personal data and purposes of processing
  - Recommended also to include consent with transfer of personal data to other group entities or service providers

Camera monitoring systems

- Two modes of monitoring
  - Without recording (online only)
    - Not considered as data processing by the Czech DPA
    - However, limitations imposed by Czech Labor Code still apply (prohibition to subject employees to monitoring without serious reasons)
  - With recording – considered as data processing
- Monitoring may only be used as a last resort
  - Only if no other, less intrusive, means of data processing may be used by the data controller
  - Limitation of the retention period – usually maximum of 72 hours
- Registration with the Czech DPA required (as with any other data processing)
- Employees must be notified via internal policy
- Monitored premises must be clearly marked
- Sufficient protection of the monitoring system and the recorded images

Czech Republic – Penalties

- Up to CZK 5,000,000 (approx. USD 251,686) for, e.g.:
  - Processing of personal data without consent, if consent is required
  - Breach of adopt sufficient security measures
  - Breach of the mandatory registration obligation
- Up to CZK 10,000,000 (approx. USD 503,373) for, e.g.:
  - Endangering a larger group of people by illegally interfering with their private and personal life caused by breach of obligations related to data processing
  - Breach of obligation related to processing of sensitive personal data (e.g. information on criminal convictions)

SQUIRE SANDERS

Slovak Republic

Slovak Republic – New Act on Protection of Personal Data

- New Act on Protection of Personal Data became effective from 1 July 2013 in the Slovak Republic (Act No. 122/2013 Coll.)
- Security of personal data – Obligation of the data controller to adopt security measures, which must be documented
  - In a security policy, if
    - personal data is processed in an information system connected with publically available computer site; or
    - sensitive personal data is processed
  - In a security project, if
    - sensitive personal data is processed in an information system and sensitive personal data is processed; or
    - the information system serves for public interest
- Authorized person
  - = every person, who comes into contact with personal data within his/her employment or function – typically statutory body (executives, directors), HR, financial director, employee doing payroll, IT employees
  - The data controller must instruct (in writing) the authorized person/s on rights, obligations and liability for breach prior to the any data processing by the authorized person

Slovak Republic – New Act on Protection of Personal Data

- Responsible person
  - If the data controller processes personal data through 20 or more authorized persons, the data controller must authorize a responsible person
  - The authorization must be done in writing
  - Deadline – 60 days from commencement of the processing
  - Requirements:
    - No criminal convictions
    - Exam taken at the Slovak Data Protection Office
  - Obligation of the data controller to notify the Slovak DPA on authorization of the responsible persons (30-day deadline)
  - Persons authorized as responsible persons under the previous law remains responsible person under the new act, however, he/she must pass the exam at the DPA by 30 June 2014

Issues:

- Few responsible persons
- Difficulties with meeting the 60-day deadline

Slovak Republic – New Act on Protection of Personal Data

- Depending on the circumstances of the data processing, one of the following is required
  - Registration with the DPA
  - Special registration with the DPA
  - Evidence by the data controller
- Registration with the DPA required for information systems, which use, even partially, automated means of data processing
  - Key exceptions:
    - Special registration is required
    - Responsible person was authorized to overview the data processing
    - Persona data are processes solely based on reasons arising from Slovak or EU law or international treaty (not based on consent of the data subject)
- Evidence
  - Data controller is obligated to keep evidence of the information system, if registration or special registration of such information system is not required

Slovak Republic – Penalties

- From EUR 300 up to EUR 5,000 for, e.g.:
  - Breach or non-fulfillment of obligation to execute a written record of instruction of the authorized person
  - Breach or non-fulfillment of obligation to execute a written record of authorization of the responsible person
  - Breach or non-fulfillment of the mandatory registration of the information system
- From EUR 1,000 up to EUR 80,000 for, e.g.:
  - Breach or non-fulfillment of obligation related to instruction of the authorized person (e.g. insufficient instruction)
  - Breach or non-fulfillment of obligation to adopt sufficient security measures in relation to protection of the personal data
  - Breach or non-fulfillment of obligation to document the adopted security measures in a security policy
- From EUR 1,000 up to EUR 3000,000 for, e.g.:
  - Breach or non-fulfillment of obligation to prepare the security project

SQUIRE SANDERS

Contact Information

Ann J. LaFrance
ann.lafrance@squiresanders.com
+44 20 7655 1752

Philip R. Zender
philip.zender@squiresanders.com
+1 415 393 9827

Karin Konstantinovova
karin.konstantinovova@squiresanders.com
+420 221 662 261