Workplace Privacy Compliance

Protection of privacy in employment relationships: the case for Costa Rica

WHY SHOULD YOU CONSIDER A WORKPLACE PRIVACY COMPLIANCE PROGRAM?

Have you considered how monitoring tools such as GPS, entrance controls, phone recording, online behavior, email use or CCTV can be implemented in the workplace? Have you thought about the use of WhatsApp groups for work purposes? Do you know if you can use information available on your employee's social media profiles? Do you have authorization to handle employees´ sensitive and health information? Do you know if you can request a background check during the hiring process?

These and many other questions are relevant from a workplace data privacy perspective. Now more than ever, a company must have clear and transparent rules on how personal information is internally processed.

By putting in place a company data protection compliance program you can make sure that you are compliant with labor laws, including the recent amendments regarding non discrimination and equal opportunities and respecting your employees right to privacy while at the same time, balancing the needs of the organization.

WHAT IS AT STAKE?

Mishandling data may trigger administrative and civil liability as well as reputational consequences.

Pro-employee decisions	• Court decisions are usually protective of the employee, and have set parameters about how employee privacy rights must be observed by the employer. Access to emails and documents, even when work related, are protected constitutionally by the right to privacy.
Labor	• From a labor law perspective, when a labor dispute arises, including dismissal situations, employees may question how their data was used.
Data Protection Authority (Prohdab)	• The Data Protection Authority (PRODHAB) can impose fines of up to USD$ 25,000 if employee data is not processed according to the law. In addition, employees have the right to claim damages in court.

An appropriate compliance program can mean the difference between a favorable or an adverse result in an employee's administrative or judicial claim.

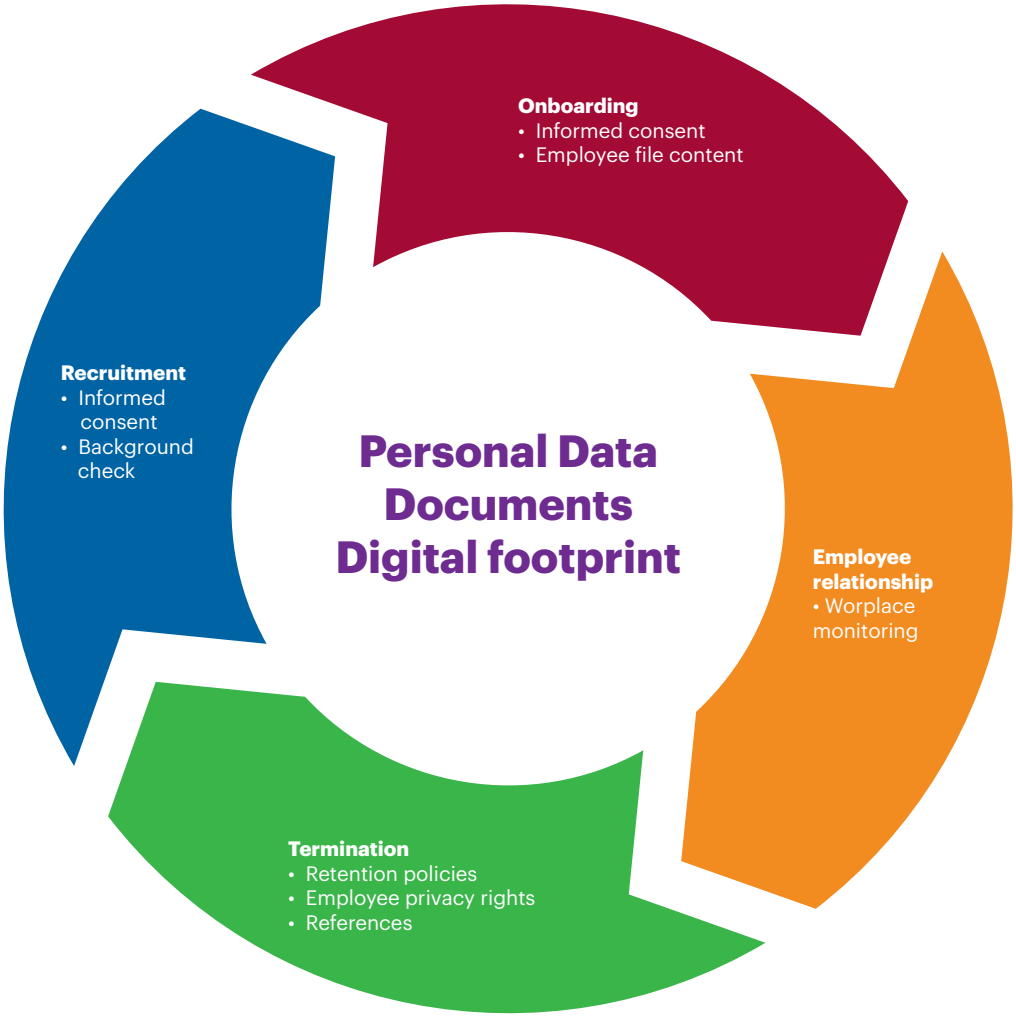
HOW TO REDUCE THE RISK

A data protection program should cover the whole lifecycle of an employee's personal data, starting with the hiring process and ending upon termination of employment. The program should consider at least:

- Informed consent or legal basis
- Background checks
- Drug and alcohol testing
- Medical information handling
- Performance and metrics evaluations
- Access to employee emails and documents
- Data retention

Because of the impact on employee privacy, monitoring activities must be carefully implemented to ensure compliance with privacy laws. All these activities trigger privacy and labor related obligations:

- Telephone recording
- Camera surveillance
- E-mail and internet monitoring
- On-line behavior: browsing, social networks and instant message services
- Access to devices used by the employee, whether personal or provided by the employer
- GPS tracking
- Biometric identity controls



STAGES AND DELIVERABLES OF A DATA PROTECTION-EMPLOYEE COMPLIANCE PROGRAM

1. Interview guidelines
2. Informed consent provisions
3. Employee file guidelines
4. Workplace monitoring guidelines
5. Termination guidelines
6. IT Policies, including BYOD
7. Training

Key contact

Monserrat Guitart, CIPP/E
Central America Regional Director
of IP and Technology
D +506 2503 9834
monserrat.guitart@dentons.com

Anna Karina Jiménez
Partner
D +506 2503 9815
annakarina.jimenez@dentons.com

CSBrand-18335 Workplace Privacy Compliance brochure CRC ENG-11 — 02/10/2019