



Data Protection in the Employment Context

Dr. Antonio Ghio
FENECH & FENECH ADVOCATES

Current Issues relating to Employment
12th October 2006

Processing of Personal Data at the workplace

- Employee data belongs to the data subject
- All Employers are Data Controllers
- Many activities in the employment context entail processing of personal data even prior to employment
- Increase in technology has increased processes
- The Data Protection Act lays down generic principles
- Applying the principles in the employment context



What data is protected? Where is it kept?

- Personal Data and Processing very broadly defined
- Surveillance and Monitoring falls under the DPA regime
- Article 3 – ‘Personal Data Filing System’ (*any structured set of personal data which is accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis*)
- Most employment records are protected



Examples of records which fall under DP realm

- Application forms and work references
- Payroll and tax information – social benefits information
- Sickness records
- Annual leave records
- Unpaid leave/special leave records
- Annual appraisal/assessment records
- Records relating to promotions/transfers/disciplinary matters
- Records relating to accident at work
- Information generated by computer systems
- Reimbursement of expenses



Interaction between Labour Law and DP Law

- Cannot operate in isolation of each other
- Interaction should assist in developments of solutions
- Protecting the workers'/data subjects' interests



DP Principles and Employment

- Finality
- Transparency
- Legitimacy
- Proportionality
- Accuracy and Retention of Data
- Security
- Awareness of Staff



Consent and Lawfulness of Processing

- Meeting the requirements of Article 9
- processing for the performance of a contract (Art.9b)
- processing for compliance with a legal obligation(Art.9c)
- **Is consent really freely given in the employment context?**



Consent and Lawfulness of Processing

Article 29 – Opinion 8/2001

“...where as a necessary and unavoidable consequence of the employment relationship an employer has to process personal data it is **misleading** if it seeks to legitimize this processing through consent. **Reliance on consent should be confined to cases where the worker has a genuine free choice and is subsequently able to withdraw the consent without detriment.**”



Processing of Sensitive Data

- **Sensitive Data** – “revealing race or ethnic origin, political opinions, religious or philosophical beliefs, membership of a trade union, health or sex life”
- In principle, explicit consent is required unless processing is necessary (exceptions):
 - complying with or exercising rights in connection to employment law (Art. 13a)
 - legal claims will be able to be established, exercised or defended (Art. 13c) (limited to actual and really prospected claims)



Surveillance and Monitoring

- DP Rules apply to surveillance and monitoring
- E-mail, Internet Access, CCTV, location data
- A proportionate response by the employer
- Relevant, Adequate and Not Excessive
- Carried out in the least intrusive way possible



Managing Employee Data

- Organisational roles and compliance mechanisms
- Understand the Law
- Perform a Data Protection Audit
- Do not process personal data which is irrelevant or excessive
- Sensitive Data
- Be aware of risks with disclosures and misuse
- Disciplinary offences for breach of DP rules
- Notifications



Job Vacancy Advertising

- Name of organisation collecting the data
- Recruitment Agencies
- Inform Applicants



The Application Process

- To whom is the data provided?
- Only Relevant Data
- Explain checks used to verify application information
- Sensitive Data
- Secure methods of sending applications



Verification of Application Information

- Inform applicants of methods used
- Obtain consent of applicants for any 3rd Party information required
- Give applicant opportunity to make representations



Short-listing and Interviews of Applicants

- Be consistent
- Automated Decisions
- Scientific Tests
- Data recorded in interviews



Pre-employment Vetting

- Only use vetting where there are significant risks involved
- At an appropriate point
- Make it clear it will take place and how it will be done
- Relevant sources – Relevant Information
- Consent



Retention of Recruitment Records

- Retention Periods on business needs
- Destroy vetting information
- What data should be transferred to employment records?
- Unsuccessful Applicants and intention to keep data on file
- Secure Storage



Collecting and Keeping General Records

- Make employees aware of what you are doing
- Inform them about the Right of Access
- Clear and foreseeable need for any information collected
- Accuracy of Records – make data subjects participate
- Accuracy, Validity and Consistency Checks



Security

- Apply Security Standards
- Access Controls
- Staff Awareness
- Audit Trails
- Control of records taken off-site
- Transmitting of data



Sickness and Accident Records

- Keep them separate
- Satisfying a sensitive data condition
- Disclosure (legal obligation, proceedings or consent)
- Make them available only to the managers responsible



Pension and Insurance Schemes

- Not intended for general employment purposes
- Limit to the maximum exchange of information with provider
- Inform the employees what information is exchanged



Marketing

- Inform the employees
- Give new workers possibility to opt-out
- Existing workers – get consent FIRST! (opt-in)
- Do not disclose data to third-party unless consented to



Fraud Detection

- Inform employees of possible use of data
- Do not disclose unless:
 - required by law;
 - in prevention or detection of a crime;
 - explicitly stipulated in the employment contract



Employees' Access to their Personal Data

- Establish systems – respond promptly
- Ensure Identity
- Provide hard-copies of information held
- Information on automated decisions
- Have technology that can assist you in retrieving data



References

- Set clear policies on who issues references
- Make sure that the data subject has consented
- Understand employees' wishes at termination of employment
- Make judgments on third-party data that might be disclosed



Disclosures

- Establish Policies – Staff Awareness
- Apply the Law if requests fall outside policies
- Legal Obligations
- Emergency Disclosures
- Third Country Transfers
- Inform data subject unless it would mean tip-off
- Keep record of non-regular disclosures and review regularly



Discipline, Grievance and Dismissal

- DP rules apply in these situations!
- Do not abuse of the data you hold and its purpose
- Establish clear procedures
- Make sure to accurately record reasons for termination



Outsourcing Data Processing

- Processors to adopt appropriate security measures
- Relationship to be governed by contract
- Third Country transfers



Retention of Records

- Establish and adhere to standard retention times
- Anonymise data where practicable
- Dispose of and Destroy effectively
- Do not keep longer than necessary



What about employers?

- Protecting the employers
- Confidentiality
- IP Considerations
- Internet and email usage policies
- Protection through strong employment contracts



Conclusion

- Employees do not leave their privacy at home
- Striking the right balance
- Employees have to accept a certain amount of intrusion of their privacy with acceptable safeguards
- No absolute answers- looking at specific circumstances in the employment relationship
- What next for Malta? Specific Regulations / Code of Practice?



Conclusion

Be a

BIG BOSS

and not

BIG BROTHER





Thank You

Antonio Ghio B.A., LL.M. Info Tech (Strathclyde), LL.D.

Fenech & Fenech
ADVOCATES

198, Old Bakery Street,
Valletta VLT09

Tel: (+356) 21 241 232

Fax: (+356) 25 990 641

Email: antonio.ghio@fenlex.com