General Data Protection Regulations and HR

21 February 2018

Agenda

1. Key Changes
2. GDPR Cradle to Grave
   - recruitment and selection
   - managing the employment relationship
   - termination and beyond
3. Case Study
4. 10 “to do’s”

GDPR – key changes

Key changes

- Core rules remain similar
- Strengthened rights for data subjects
- Less reliance on “consent”
- Concept of “high risk” processing
- Data processors as well as data controller obligations
- Breach consequences

General principles

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Retention
- Integrity and confidentiality

Key change – breach and sanction

Penalties

• up to 4% global turnover or 20 million (whichever higher)

Breach notification

- To regulator “without undue delay” and within 72 hours where “risk” to data subject
- To data subject where “high risk”
- Importance of encryption; regular systems testing

Key change – consent

- must identify “processing condition”

  - Consent
  - Necessary for performance of contract
  - Legal obligation
  - Vital interest of data subject
  - Public functions
  - Legitimate interests

- much harder to rely on consent in employment context – freely given, specific, informed, unambiguous….

Key change – strengthened rights for data subjects

- Right to be informed – Privacy Notices
- Right of access - subject access rights (30 days, no fee, “manifestly unfounded or excessive”)
- Right to be forgotten – not absolute
- Rights relating to automated decision making

Key change – governance and accountability

- Data Protection Officers
  - mandatory for public bodies and if processing is core business activity
  - independent, expert and senior
  - DPOs will have additional employment protections
  - Be wary of titles!
- Data protection by design
- Data protection impact assessment

GDPR Cradle to Grave – recruitment and selection

Recruitment and selection – Application Process

- **Data minimisation**
  - only ask for information that is necessary
- **Consent**
  - Unlikely to be able to rely on blanket consent
  - Consent must be “freely given”
  - Consent can be withdrawn at any time
  - Need to look for processing to be justified on other legally-recognised grounds (see later)

Recruitment and selection – Application Process

- **Privacy Notices**
  - Concise / transparent / intelligible / easily accessible and in clear and plain language.
  - In writing / electronically (if appropriate) and orally in some cases.
  - Must be provided at the time of data collection from either data subject or a third party

Privacy Notice

- Your identity and contact details and details of DPO
- Purpose and legal basis for processing and *period that it will be stored*
- *Right to withdraw consent*
- Categories of personal data processed and the source of the data
- Recipients of the personal data and details of any intended transfer outside the Union
- *Individuals rights e.g.right to be forgotten, to make subject access request*
- Details of any automated decision making
- *Whether provision of personal data is a statutory or contractual requirement.*
- *The right to complain to a supervisory authority*

Recruitment and selection – Application Process

- **Access NI: Criminal Record Checks**
- **Document Security**
  - Pseudonymisation and encryption of personal data
  - Ability to ensure on-going confidentiality and resilience of data processing systems
  - Demonstrate how you test your security systems and assess how well they are working / identify issues

Recruitment and selection – Application Process

- **Beginning the employment relationship**
  - Audit documentation that you currently hold
  - Send new (more detailed) Privacy Notice
- **Retention of documents**
  - Suggested periods (next slide)
  - Consider legal basis for processing data:
    - Performance of employment contract
    - Compliance with legal obligation
    - Protect employers vital interests
    - For a task carried out in the public interest
    - For the purposes of the legitimate interests of the employer (or third party)

Retention of records- recruitment

Type of record	Suggested Legal Basis for processing	Statutory or Code of Practice reference	Retention period
Job applications and interview records of unsuccessful candidates	Performance of the employment contract	ICO: Employment Practices Code	A short period, perhaps 6 months after notifying unsuccessful candidates
Fair employment monitoring information from unsuccessful candidates	Compliance with a legal obligation	Fair Employment and Treatment (NI) Order 1998	3 years from the date of receipt of the unsuccessful application
Records to show compliance with the Working Time Regulations (NI) 2016 (including opt-out forms)	Compliance with a legal obligation	Working Time Regulations (Northern Ireland) 2016	Potentially for the length of the employment relationship and appropriate period beyond e.g. 6 months
PAYE records	Performance of the employment contract	Regulation 97 Income Tax Regulations 2003	Not less than three years after the end of the tax year to which they relate

Retention of records

Type of record	Suggested Legal Basis for processing	Statutory or Code of Practice reference	Retention period
Immigration checks	Compliance with a legal obligation	Immigration, Asylum and Nationality Act 2006	Two years after the termination of employment
Criminal records checks and disclosures of criminal records forms	Compliance with a legal obligation	ROA and Information Commissioner's Employment Practices Code Part 1.7.4 and 2.15.3	Delete following recruitment process unless assessed as relevant to ongoing employment relationship. Once the conviction is spent, should be deleted unless an excluded profession.

GDPR Cradle to Grave – managing the employment relationship

Disciplinary / performance

- The right to be forgotten
- Subject access requests
  - Enhanced rights
  - Removal of £10 fee
  - Response without “undue delay” and within one month
- Tougher data protection rules – ‘a two way street’
  - Removal or misuse of confidential information
  - Review of disciplinary policy

Managing sickness absence

- Sickness absence records
  - Right to be forgotten
  - Retention of records
- Reporting of sickness absence
  - Review of reporting procedures
  - Sharing of information

Managing sickness absence

- Occupational Health Records
  - Consent - “specific, informed and unambiguous”
  - Separate privacy notice
  - Employee’s right to object to processing
  - Audit of “necessary data”

Privacy Impact Assessments

- What type of information is being held? What's the risk of that information being lost?
- Automated decision making
  - Extensive and systematic profiling
    - Performance management / triggers for sickness absence
    - Eligibility for attendance bonuses
- Systematic monitoring
  - CCTV
  - Biometric access controls
  - Tracking devices
  - Email and internet monitoring

Retention of records

Type of record	Suggested Legal Basis for processing	Statutory or Code of Practice reference	Minimum Retention period
Disciplinary / grievance / performance records	Performance of the employment contract	N/A	At least until the expiry of any warning. Suggest regularly reviewed as part of an audit process.
Sickness records required for the purposes of SSP	Compliance with a legal obligation	Regulation 13, Statutory Sick Pay (General) Regulations 1982	Three years after the end of the tax year in which payments are made
Records in relation to hours worked and payments made to workers	Compliance with a legal obligation	Section 9, National Minimum wage Act 1998. Regulation 38, National Minimum wage Regulations 1999	Three years beginning with the day upon which the pay reference period immediately following that to which they relate ends

GDPR Cradle to Grave – termination and beyond

Termination and beyond

- **Document audit**
  - Consider what can be destroyed and what should be retained
- **Employees removing personal data**
  - Potentially uploading information or using it to compete
  - Mandatory reporting to ICO and potentially data subject
- **Reference requests**
  - Reason for processing?
  - Exit interview / consent
- **Subject Access Requests**

GDPR – Case study: before and after

Morrisons supermarket

- Mr Skelton employed by Morrisons as Senior IT internal auditor
- Subjected to disciplinary procedure in July 2013
- In November 2013, as part of his role, he obtained personal information (payroll data) and forwarded to auditors. He also transferred it to personal USB stick
- In January 2014, before annual financial reports announced, details of 100,000 employees posted on a file sharing website by S. He had used another employee's details to open an account.
- March 2014 – arrested and charged with fraud
- July 2015 – sentenced to 8 years in prison
- Group civil action against Morrisons
- Morrisons held to be vicariously liable.

GDPR – “to do” list

GDPR – getting ready

- Audit employee data currently held by the business – what, where, why?
- Determine whether you are required to formally designate a Data Protection Officer.
- Review Privacy Notices and Procedures.
- Identify the relevant processing condition; document this carefully
- Review and update contracts of employment and policies

GDPR – getting ready

- Consider and implement procedures for detecting, reporting and investigating breaches
- Update procedures for dealing with subject access requests
- Update procedures for assessing and reporting breaches
- Consider data protection training for all staff as part of induction and at regular intervals

CARSON McDOWELL

Any questions?

Northern Ireland's Leading Law Firm

- Regional Law Firm of the Year, Legal 500 2016, – the second time the firm has won the award in the past three years.
- Northern Ireland's Top Ranked Law Firm in the Chambers and Partners Guide 2017 for the past number of years.
- More areas and partners ranked than our competitors.

We do more. Better.