DAC beachcroft

# The General Data Protection Regulation: What Employers Need to Know

Kate Galloway & Nicola Geary

28 September 2017

# GDPR: The Headlines

- Will come directly into force on 25 May 2018
- Purpose: to introduce common standards across EU
- Increased penalties for non-compliance (4% global net turnover or EUR 20,000,000, whichever higher)
- Government has just published a draft Data Protection Bill confirming:
  - Data Protection Act 1998 will be repealed
  - GDPR will be implemented regardless of Brexit
- Aim is to ensure uninterrupted transfer of data between the UK and EU following Brexit for trade and law enforcement purposes

# GDPR: Key Themes

DATA PROTECTION PRINCIPLES AND INTERNATIONAL TRANSFER REGIME LARGELY UNCHANGED

**ACCOUNTABILITY**

privacy impact assessments

privacy by design/default

appointment of DPOs

**BROADER SCOPE**

obligations on data processors

expanded territorial scope

**SECURITY**

obligations to notify breaches

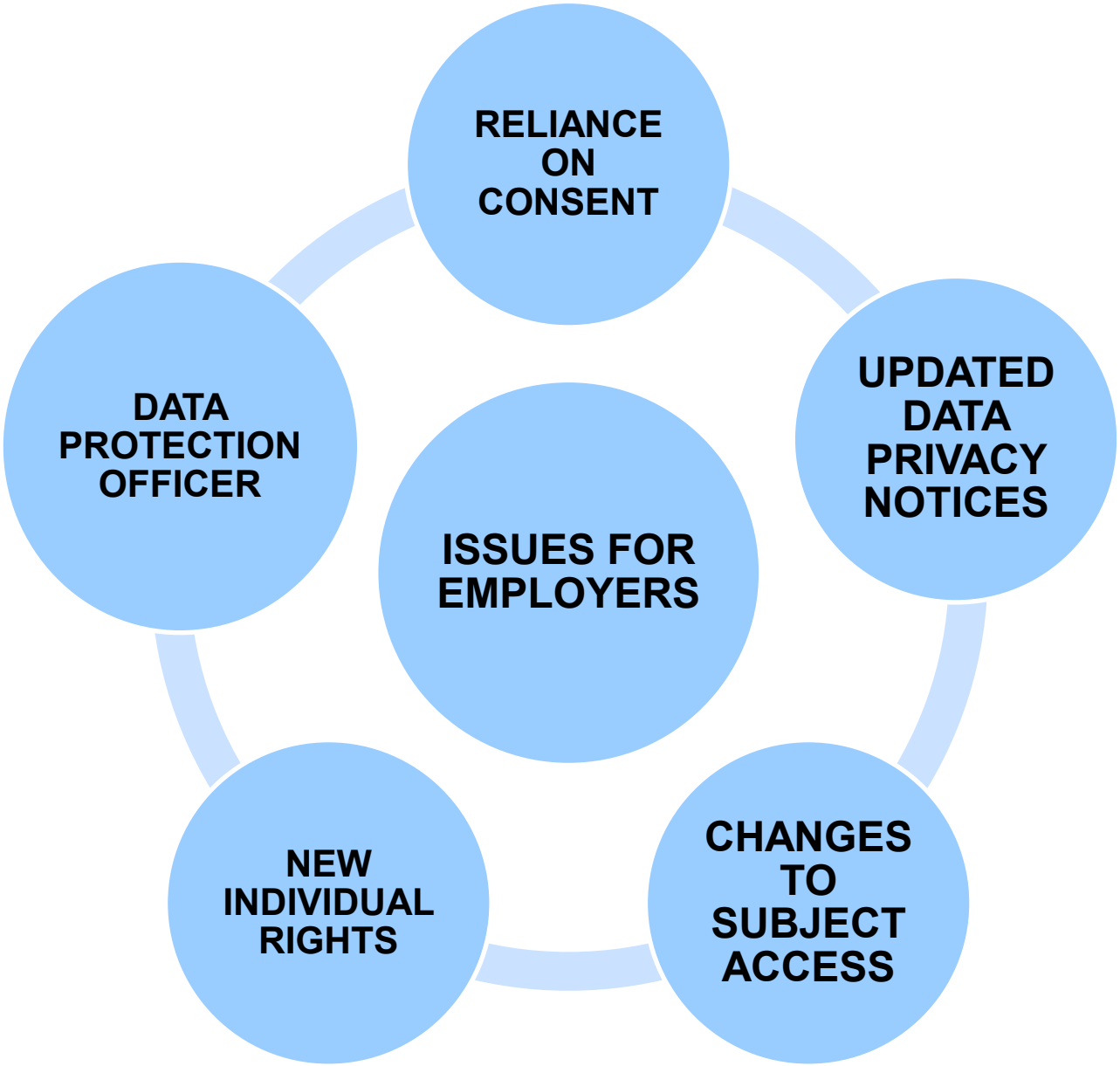
recognition of "pseudonymised" data

**SUBJECT RIGHTS**

right of data portability

enhanced right of erasure

right to object to profiling


RELIANCE ON CONSENT
UPDATED DATA PRIVACY NOTICES
CHANGES TO SUBJECT ACCESS
NEW INDIVIDUAL RIGHTS
DATA PROTECTION OFFICER
ISSUES FOR EMPLOYERS

# Reliance on consent

- **DPA 1998 & ICO Guidance**
  - Valid consent is challenging in the employment context
  - Employers should rely upon other conditions

- **GDPR**
  - Higher standard for consent
    - Freely given, specific, informed and **unambiguous** indication **by a statement or by a clear affirmative action**
    - Consent request should not be part of your terms and conditions
    - Requires positive opt-in and ability to withdraw

# Alternatives to Consent

## ORDINARY PERSONAL DATA

- Necessary for performance of (employment) contract
- Compliance with legal obligation
- Pursuit of legitimate interests (without undue prejudice)

## SENSITIVE PERSONAL DATA

- Performance of right or obligation imposed by law in connection with employment
- Equal opportunities monitoring

# Criminal Records: No overall changes

- **DPA 1998**
  - Included in definition of sensitive personal data
  - Rely on specific requirements for certain roles (e.g. regulated roles)

**GDPR**

- Not in definition (consent will not help)
- UK derogations for exercising employment law obligations / criminal convictions data

# Reliance on consent: ACTIONS

- ✓ Remove consent clauses from template employment contracts
- ✓ Audit processing of ordinary and sensitive personal data to confirm other conditions for processing apply
- ✓ Seek consent only where truly needed where other conditions do not apply
- ✓ Comply with GDPR requirements where consent is sought

# Data Protection Policies

- **DPA 1998 & ICO Guidance**
  - Publish high level information to employees, contractors, job applicants about processing
  - General principle of transparency

- **GDPR**
  - Detailed requirements around privacy notice
  - Must be concise, transparent, easily accessible and given in plain language

# Notice Requirements

- Identity and contact details of data controller
- Categories and source (unless employee is the source)
- Purposes and legal bases for processing – if legitimate interests, these must be specified
- Recipients or categories of recipients
- The period the data will be stored
- Data subject rights: access, rectification, erasure, objection, portability and ability to complain to the regulator (with contact details)
- The legal basis for transfer to a non-EU country

# Data Processors (1)

- GDPR imposes specific and separate duties and obligations on data processors
- Employers may typically use data processors in context of payroll and benefits provision
- Data controller required to enter into contract with data processor to impose certain obligations to safeguard data subjects

# Data Processors (2)

- Obligations on data processors include:
  - security arrangements equivalent to data controller;
  - to only process data on documented instructions of data controller; and
  - to employ staff who are under confidentiality obligations.
- Data processors have own liability under GDPR for non compliance
- May complicate arrangements between data controllers and data processors and result in processors wanting greater clarity on their responsibilities

# Data Protection Notices: ACTIONS

Update:

- ✓ Employee Data Protection Notice
- ✓ Contractor / Third Party Data Protection Notice
- ✓ Recruitment Privacy Notice (for job applicants)

# Subject Access Requests: Key Changes

- Abolition of £10 fee – exceptions:
  - "Manifestly unfounded or excessive" requests, particularly if repetitive – can charge reasonable fee for admin costs / decline to respond
  - Requests for further copies of the same information

- Reduction in response period from 40 days to "without delay" and at the latest within 1 month
  - Time period extendable by additional 2 months where requests complex/numerous

# Subject Access Requests: Key Changes

- Right to information including:

| | |
|---|---|
| Purposes of processing | Individual's rights* |
| Categories of data | Right to complain* |
| Recipients | Information as to third party sources* |
| Envisaged period of data storage* | Existence of profiling* |

(* New requirements)

- Best practice recommendation to provide remote access to data on a secure system
- ICO still planning to operate a pragmatic approach

# Practical Steps: (1) Targeting the Search

- Can require evidence to confirm identity
- Can require information to locate the data being sought:
  - individuals involved in processing
  - types of files/documents
  - relevant date ranges
  - key words or topics
- Delays timescale for compliance until receipt of information

# Practical Steps: (2) Narrowing the Search

- Approach to search exercise: what is reasonable?
  - individuals / IT/HR / IT cyber forensic team
- Scope to limit search of individual's e-mails if:
  - searches are unlikely to reveal personal data
  - relevant e-mails will be picked up in other searches
- Archived data: scope to conduct highly targeted searches based on relevant information
- Deleted data: scope to exclude altogether if reconstitution will require significant time and effort
- Manual searches generally excluded unless highly structured

# Practical Steps: (3) When is Data "Personal"?

Impact of *Durant* and subsequent ICO Guidance has significantly narrowed what information will amount to "personal data"

## INCLUDED

- e-mails relating to personal or family life
- expressions of personal opinion
- calendar entries showing individual's location

## EXCLUDED

- all day to day business communications inc e-mails
- content of meeting minutes
- individual's expressions of opinion/belief on behalf of employer

# Subject Access Requests: ACTIONS

- ✓ Devise protocol for SAR response if face frequent requests
- ✓ Provide training (i) to spot requests; and (ii) responding promptly
- ✓ Ascertain IT capability around retrieval of archived and deleted electronic data – so can determine when to rely upon exceptions for (i) burdensome requests; and (ii) manifestly unreasonable requests


erasure
objection
rectification
OTHER RIGHTS
profiling
portability

# Mandatory Appointment of DPO

- **Scope**
  - Public bodies; and
  - Organisations who control large data sets for their core business i.e. large organisations
- **Duties**
  - Self-regulating role – report to highest level of management / maintain significant independence
  - Ensure regulatory compliance, staff training, co-ordinating with regulators
- **Protected employment status** – no dismissal / detriment for performing tasks

# Housekeeping Checklist

- basic training for employees on their obligations
- security procedure for transmission or transportation of data e.g. using encryption
- transfer agreements in place with any recipients of data
- data retention policy – implemented on regular basis to purge employee records of data which is no longer needed

# Any questions?

# Your speakers – contact details

**Kate Galloway: Legal Director**

**DD: 020 7894 6261**

**Email: kgalloway@dacbeachcroft.com**

- Kate is a senior employment lawyer who provides strategic advice on a range of employment law issues and who specialises in defending complex and high value discrimination and whistleblowing cases.
- Kate has a particular interest in data protection issues and in the implementation of the GDPR. She has regularly advised clients on subject access requests in the context of litigation and difficult employee relations issues.

**Nicola Geary: Associate**

**DD: 020 7894 6745**

**Email: ngeary@dacbeachcroft.com**

- Nicky has experience of a range of non-contentious and contentious employment work, predominantly in the financial services and insurance sectors. Nicky regularly advises clients on data protection issues, giving practical advice on how to handle onerous subject access requests including during her recent secondment to the in-house employment legal team of an investment bank.
- During her career Nicky has also undertaken secondments in the in-house legal team of a large financial services organisation and to a Speciality Claims team of a global insurance company.

DAC beachcroft