WEBINAR

SHOOSMITHS

Employment webinars series 2024 | Protecting employee data

This webinar will begin at 10:00

FOR WHAT MATTERS

Connect with your speakers on LinkedIn

Gwynneth Tan

PARTNER

Stuart Lawrenson

PARTNER

SHOOSMITHS

Protecting Employee Data

Protecting your employee brand

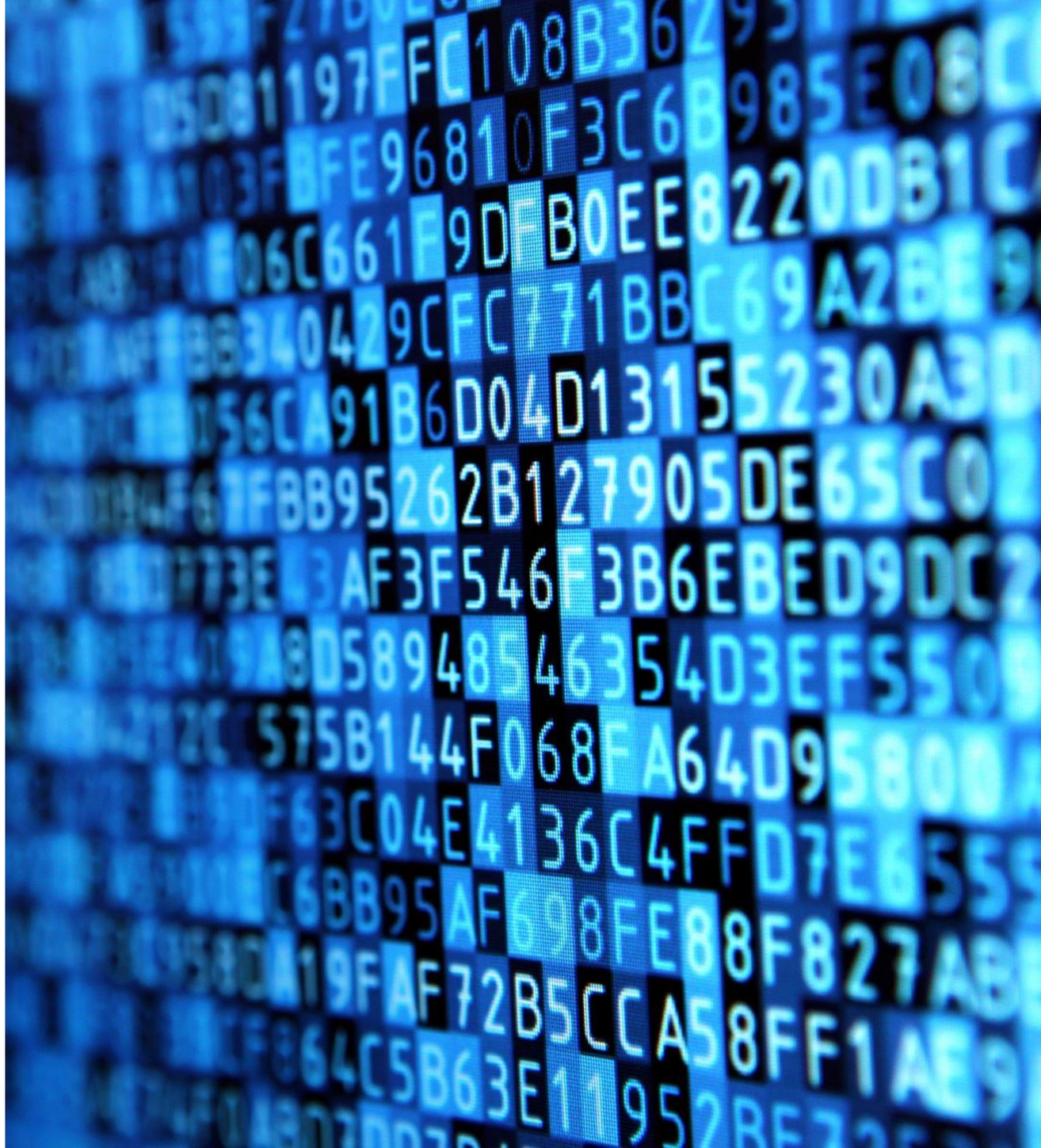
Gwynneth Tan
Partner

Stuart Lawrenson
Partner

FOR WHAT MATTERS

Agenda

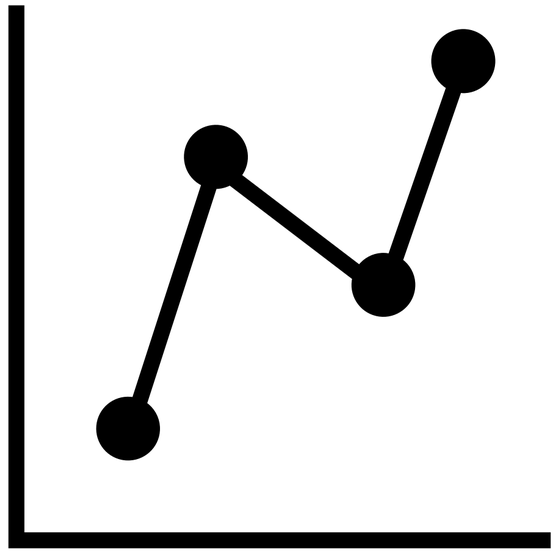
- ICO 3 year plan ‘ICO25’
- Recap of key data protection principles
- Employee monitoring and use of AI
- Handling employee DSARs effectively
- Controlling the use of social media



ICO Approach

ICO25

- ICO approach
  - Safeguarding vulnerable
  - Empowering organisations and employees
  - Emphasis on trust



Data Protection: Key Principles

Accountability

Fair and lawful

Purpose limitation

Storage limitation

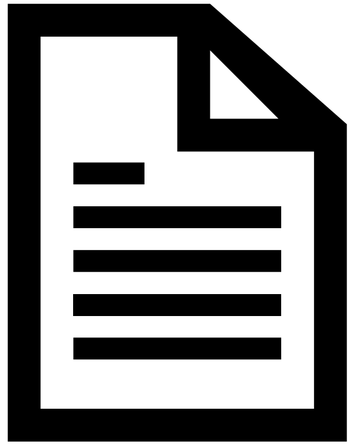
Data minimisation

Integrity and confidentiality

Accuracy

Transparency

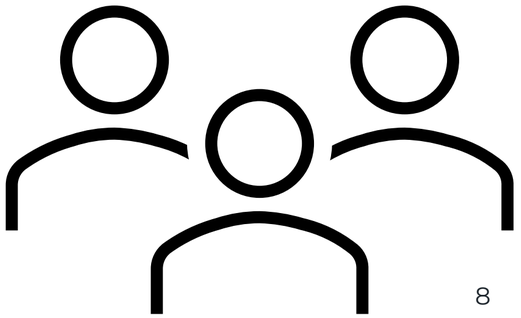
New Guidance



- The Employment Practices Code consisted of 4 parts:
  - Recruitment and selection
  - Employment records
  - Monitoring at work
  - Information about workers' health
- Replaced by ***Employment practices and data protection: monitoring workers*** and ***Information about Workers Health*** to provide greater certainty and protection to employees on their data protection rights
- ICO has also issued additional guidance on AI and Biometric Data

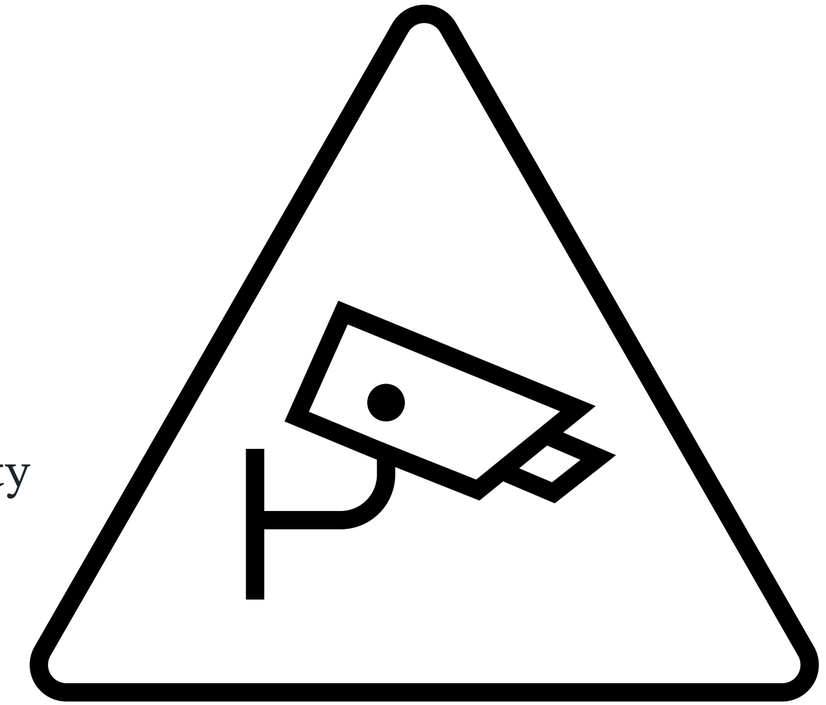
ICO Guidance: Employee Monitoring

- Aimed at employers and provides guidance on monitoring workers lawfully, transparently and fairly
- Employers encouraged to consider legal obligations and workers' rights **before** implementing any monitoring in the workplace
- Scenarios for different ways of worker monitoring
- Data protection checklists provided as a quick overview/guide to help employers think about what needs to be considered



Employee Monitoring

- Purpose?
- Legal basis?
- Necessary, justified and **proportionate**?
- Processed **fairly**, lawfully and in transparent manner
- Data Protection Impact Assessment (**DPIA**)
- **Inform** employees – limited exceptions (covert monitoring)
- Human Rights Act 1998 – reasonable **expectation of privacy**
- **Artificial intelligence** (e.g., biometric monitoring and productivity monitoring)



Biometric Data : ICO Guidance

- Biometric data is "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data" (Article 4(14), UK GDPR).
- Biometric recognition : when biometric data is used to uniquely identify someone
- ICO guidance explains how data protection law applies to biometric data in biometric recognition systems
- Aimed at organisations that use, or are considering using, biometric recognition systems and for providers of these systems

Using Biometric Data for Monitoring: ICO Guidance

- To process biometric data lawfully:
  - identify a lawful basis and a separate condition for processing special category biometric data before you begin processing
  - complete a DPIA before you use a biometric recognition system
  - Ensure systems in place to correct inaccurate information
  - Update privacy notice
  - Ensure appropriate security measures, such as encryption or access restrictions

Biometric Data: Enforcement Action

- The ICO took enforcement action taken against **Serco Leisure**
- Biometric data of more than 2,000 employees at 38 leisure facilities was unlawfully processed
- Employees were not offered a clear alternative
- By 19 May 2024 Serco must:
  - stop using facial recognition technology to monitor employee attendance
  - destroy all biometric data and all other personal data that Serco is not legally obliged to retain

SHOOSMITHS

Handling employee DSARs effectively

FOR WHAT MATTERS

Recent developments and top tips

- What is a DSAR?
- What is the right of access?
- How to recognise a DSAR
- Initial considerations
- Timings
- When you can refuse finding and retrieving data
- Exemptions
- Redactions
- How data should be provided
- Preparation for and practical steps

Recent developments

- What we are seeing
- What we are doing!
- New guidance from the ICO “Subject access request Q and A’s for employers”
- ICO Portal…now easier than ever to make a DSAR
- ICO Guidance 2023
- Updated guidance on timescales…
  - Day of receipt – day one (not the day after)
  - e.g. DSAR received on 14 May has to be responded to by 14 June

What is a DSAR?

- A DSAR is a data subject access request which can be requested by employees who exercise their right of access
- When a DSAR is requested, an individual is only entitled to their own personal data – not to information relating to others

What is the right of access

Gives the individuals the right to obtain:

i. Confirmation you are processing their data
ii. A copy of their personal data
iii. Other supplementary information

How to recognise a DSAR

How are requests made?

- In writing, by email, or other electronic means
- Can be made on social media
- Can be verbal

Scope of request

- Framed widely
- Does not need to refer to the GDPR or DPA
- No right to see ‘documents’, only their personal data

Requests made on behalf of others

- Via a third party

Initial considerations

- Individuals are only entitled to **their own** personal data (unless they are acting on behalf of another individual)
- Check identity of person making request
- Make an initial assessment
- Clarification of a request
- Charging fees

How long have you got to respond

- You must comply with a SAR without undue delay and at least 1 month of receipt of the request
- Time limit begins from the day you receive the request until the corresponding calendar date the next month
- If the corresponding date falls on a weekend or public holiday you will have until the next day to respond
- If clarification is requested the time limit for responding is paused until clarification is obtained

Refusing to comply with a SAR

A request can be refused if:

- An exemption applies
- The request is manifestly unfounded or excessive

When is a request manifestly unfounded or excessive:

- Repetitive requests may be excessive
- Manifestly can be interpreted as “obviously” or “clearly”
- Excessive is likely to be interpreted with the principle of proportionality
- The individual’s purpose and motivation may be relevant
- You are able to charge a reasonable fee or refuse to act
- Do not be too quick to say that a request is unfounded or excessive though!

Finding and retrieving relevant information

- Businesses should make reasonable and proportionate efforts to retrieve information
- Consider if other information is needed from the individual to help with locating information
- How to retrieve information from differing sources:
  - Electronic records not easily available
  - Archived information and back-up records
  - Deleted information
  - Information contained in emails
  - Information stored in different locations
  - Information stored on personal computers
  - Personal data in big data sets
  - WhatsApp messages
  - Deleting or amending data

When do exemptions apply

There is no obligation to comply with a DSAR in relation to:

- **Confidential references**
- Publicly available information
- Crime and taxation
- **Management forecasting or management planning**
- **Negotiations between the employer and employee**
- Regulatory activity
- **Legal advice and proceedings**
- Social work records
- Health and education records

Redacting data

- Can be used to protect the identity of another individual
- Can be used to remove information which is out of scope
- Seek advice on how to save documents to ensure there is no risk of the individual being able to delete the blacked-out sections
- Ensure to keep original non-redacted copies of documents

How should the information be supplied to the requester?

- How to decide what information to provide
- What format should we provide the information
- Do we need to provide remote access?
- Does the company have to explain the information supplied

What goes into the response?

- Supply a copy of the personal data concerning the individual
- In addition, you must also provide:
  - Purposes of the processing
  - Categories of personal data
  - Recipients or categories of recipient
  - Source of personal data
  - Retention periods
  - Existence of automated decision making (including profiling)
  - Transfers outside the EEA and safeguards
  - Existence of data subject rights
  - Right to lodge a complaint with ICO

How should business prepare for a DSARs

Ways in which businesses can prepare for SARs:

- Training
- Guidance for staff
- Appointing staff members to deal specifically with requests
- Asset registers
- Checklists
- Logs
- Retention and deletion policies
- Security
- Rectification of data to ensure data held is accurate. Incorrect information could lead to disputes and unlawful deduction.

Practical steps

- Use a data room to facilitate document review (creates audit trail)
- Diarise the deadline to reply
- Narrow the scope of request if possible
- Consider whether the request is manifestly unfounded or excessive
- Consider extending the time to respond (this can be up to 3 months)
- Consider exemptions
- Wrap up in a settlement agreement
- If in doubt – seek legal advice!

DSAR: Case law

- ***FF v Österreichische Datenschutzbehörde and CRIF GmbH C-487/21***
  - the individual must be provided with a "*faithful and intelligible reproduction of all those data*"
- ***RW v Österreichische Post AG C-154/21***
  - where personal data has been, or will be, disclosed to third parties, the identity of the recipients must be disclosed to the individual on request

SHOOSMITHS

Protecting your business social media

FOR WHAT MATTERS

Recent developments

- What we are seeing
  - Significant increase in queries
  - Issues arising both during and post-employment ending
  - Numerous requests for assistance with Social Media policies

Social Media policies – drafting considerations

- What other policies should your Social Media policy refer to?
- Do you allow any personal use of social media during work?
- How are you going to define prohibited use?
- Will employees be required to use social media for business use?
- Useful to include acceptable use guidelines
- Sensible to have ability to monitor
- Do you use for recruitment?
- What are the consequences of breach

NB: Data on Social Media can = personal data!

Your contacts

Gwynneth Tan

PARTNER

T +44(0)3700 868477

M +44(0)7718 037127

E Gwynneth.Tan@shoosmiths.com

Stuart Lawrenson

PARTNER

T +44(0)3700 866733

M +44(0)7595 096587

E Stuart.Lawrenson@shoosmiths.com

SHOOSMITHS

FOR
WHAT
MATTERS