WEBINAR

Welcome

Employment Webinar

DSARs and other practical data protection issues for employers

SHOOSMITHS

WEBINAR

Your hosts

Connect with your hosts on LinkedIn by scanning the relevant QR code below.

Michael Briggs, Partner

michael.briggs@shoosmiths.co.uk

Adele Hayfield, Partner

adele.hayfield@shoosmiths.co.uk

Gwynneth Tan, Partner

gwynneth.tan@shoosmiths.co.uk

Overview

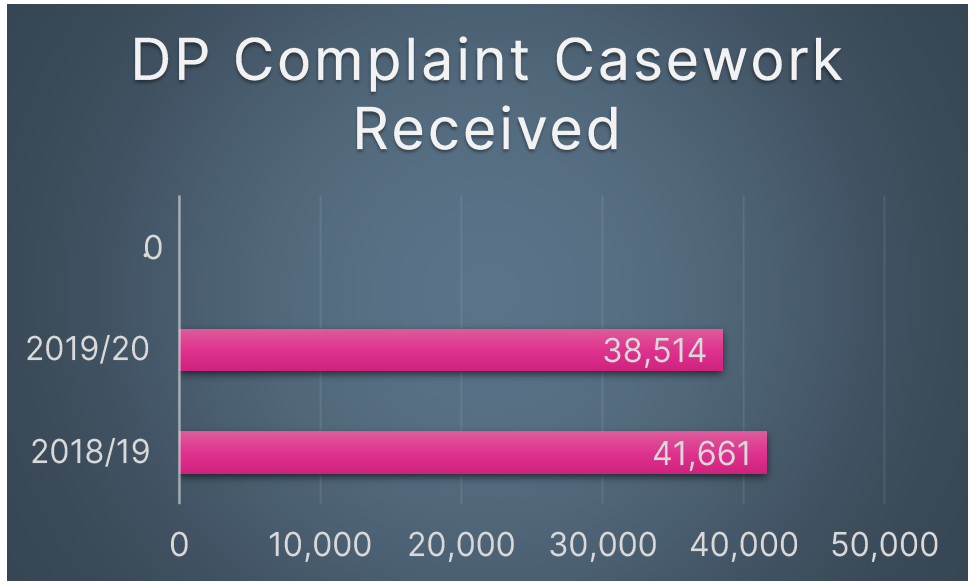
- Post Brexit Data Protection Law
- Key Statistics and Cases
- What are DSARs and how to handle them?
- Updates to ICO guidance on DSARs
- Data Breaches and their consequences

Post Brexit Data Protection Law

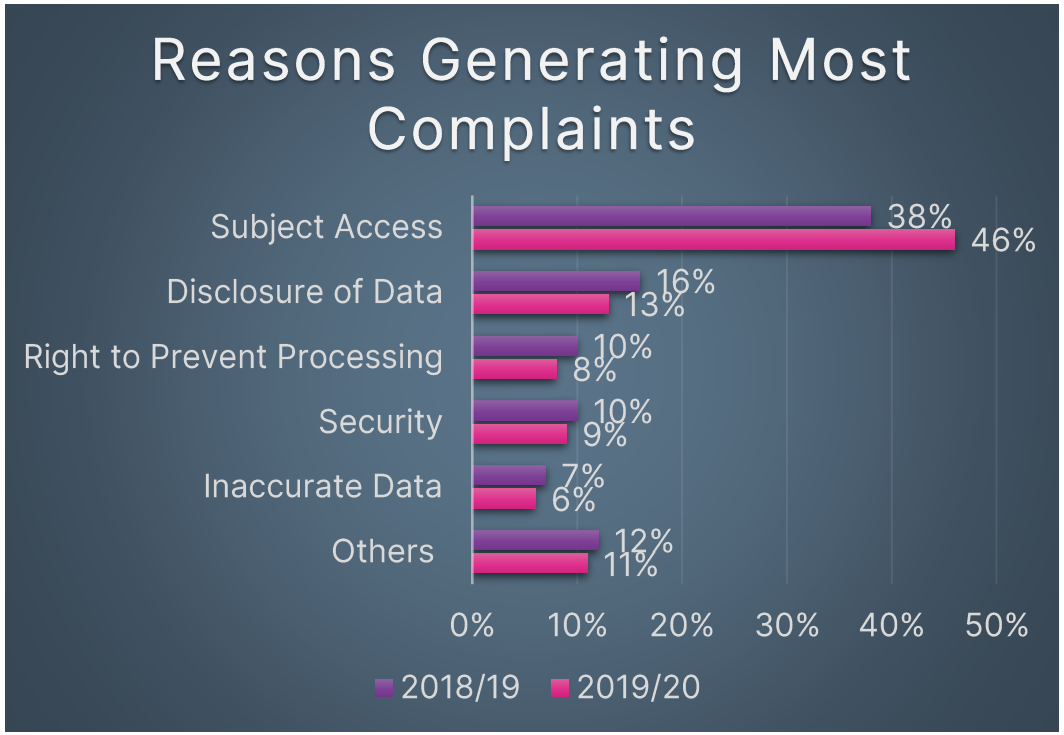
- GDPR has been retained and continues to apply in the UK
- Data Protection Act 2018 continues to apply
- The key principles, rights and obligations of data protection remain the same
- Personal data can be transferred from UK to EEA
- Personal data can be transferred from EEA to UK until 30 April 2021 – UK is awaiting confirmation from EC regarding adequacy decision

Complaints to the ICO

Graph 1



Graph 2



Data sourced from the ICO

Enforcement by the ICO

Hudson Bay Finance Ltd

- Enforcement Notice for failure to comply with DSAR
- Failed to comply with requests & Preliminary Notice from ICO

Magnacrest Ltd

- Criminal proceedings for failure to comply with Enforcement Notice
- Fined

Other Fines

- British Airways - £20m for customer data breaches
- Marriot International - £18.4m for failure to keep personal data secure
- Ticketmaster - £1.25m for failure to keep customers' payment details secure

What is a DSAR?

- DSAR = Data Subject Access Request
- The right of access (i.e. subject access) gives individuals the right to obtain a copy of their personal data
- Personal data is any information where an individual can be directly or indirectly identified from it
- An individual is only entitled to their own personal data – not to information relating to others
- An individual is 'identified' or 'identifiable' if you can distinguish them from other individuals

Recognising a request

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

Poll – Please answer

1. How many DSARs do you receive per year?
2. Do you handle DSARs internally or outsource them?
3. Do you receive stand alone DSARs or DSARs with an Employment Tribunal claim or grievance?

Responding to a request

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

Timings

- Respond without undue delay
- Within 1 month
- Extension to 2 months for complex/numerous requests

Manifestly unfounded or excessive requests

- It seems reasonable to assume that:
  - 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!

Updates to ICO guidance on DSARs

In October 2020, the ICO updated their right of access guidance to include further clarification on complex areas of law and to provide more practical examples. The three main topics clarified in the ICO update are:

(1)

Stopping the clock for clarification

(2)

What is a manifestly excessive request?

(3)

What can be included when charging a fee for excessive, unfounded or repeat requests?

Finding the personal data

- You may ask the individual to clarify their request and provide additional details to help locate the information
- Cannot require the individual to narrow the scope of their request … but you can ask
- Can ask for information to help you locate the requested information
- Emails are a good starting point
- Other places to look:
  - Backed up data
  - Deleted data
  - Data held on other systems

Changes to data

- A DSAR relates to data held at the time the request was received
- The use of some data may result in it being amended or deleted whilst you are dealing with the request
- Reasonable to supply the information you hold when you send out the response – even if this is different to what was held when you received the request
- DO NOT delete any data to defeat a DSAR!

Third party data – 3 step approach

1. Does the request require disclosure of information that identifies another individual?

2. Has the other individual consented?

3. Would it be reasonable to disclose without consent?

Exemptions

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

- Confidential references
- Publicly available information
- Crime and taxation
- Management information
- Negotiations with the requester
- Regulatory activity
- Legal advice and proceedings
- Social work records
- Health and education records

Formal Response to the DSAR

- 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

Challenges to DSAR response

- An individual may challenge the response:
  - Complain to the ICO
  - Apply to a court for a compliance order
  - Civil claim for damages

Practical Tips

- Reduce data you hold – robust system of retention/deletion
- Have a DSAR policy in place and a standard request form (although cannot make it compulsory to complete)
- Use data room to facilitate review (creates audit trail)
- Record details of requests you receive
- Train staff to deal with a request

Practical Tips

- Diarise the deadline – consider extending time
- Narrow the scope of request if possible
- Consider whether manifestly unfounded or excessive
- Consider exemptions
- Wrap up in a settlement agreement

What is a Data Breach

> A security incident that has affected the confidentiality, integrity or availability of personal data

Includes both deliberate and accidental breaches

What should you do?

- Establish if breach has occurred
- Take steps to address/contain it
- Establish severity of risk to people's rights & freedoms
- Tell the ICO if required

Notifications after breach

Deciding whether to notify the ICO

> *You must notify the ICO if the breach is likely to result in a risk to rights and freedoms of data subject*

- Type of breach
- Nature, sensitivity and volume of personal data
- Ease of identification of data subject
- Severity of risk to data subject
- Number of affected individuals
- Special characteristics of data subject/controller

Timescales

- Report to the ICO within 72 hours
- Report to data subject without undue delay if risk is high

Consequences of Data Breach

1. Physical, material or non-material damage to data subject
   - Identity theft or fraud
   - Financial loss / reputational damage
   - Loss of confidentiality

2. Damage to data controller
   - Financial loss
   - Reputational damage