Veale Wasbrough Vizards

Data protection training

The Rubicon Network, February 2015

Andrew Gallie

www.vwv.co.uk | Offices in London, Bristol & Birmingham
Lawyers & Parliamentary Agents

Veale Wasbrough Vizards

Part 1: data protection essentials

Veale Wasbrough Vizards

An overview of the Data Protection Act 1998

- Protects an individual's rights in respect of their information (eg a right to privacy)
- Requires organisations to comply with the eight data protection principles which cover issues such as fairness, security, and retention periods
- Gives individuals certain rights in their data such as a right to request a copy of the personal data which the organisation holds about them (a subject access request)
- Regulated by the Information Commissioner
- Sensitive personal data: racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health or condition, sexual life and actual or alleged criminal activity

Veale Wasbrough Vizards

The eight data protection principles

1. Processed fairly and lawfully
2. Obtained and used for specified and lawful purposes only
3. Adequate, relevant and not excessive in relation to their purposes
4. Accurate and up-to-date
5. Not kept for longer than is necessary
6. Processed in accordance with the individual's rights
7. Kept secure
8. Not transferred outside of the EEA without adequate protection

Veale Wasbrough Vizards

Q1 A breach of which principle is treated most seriously?

1. Processed fairly and lawfully
2. Obtained and used for specified and lawful purposes only
3. Adequate, relevant and not excessive in relation to their purposes
4. Accurate and up-to-date
5. Not kept for longer than is necessary
6. Processed in accordance with the individual's rights
7. Kept secure
8. Not transferred outside of the EEA without adequate protection

Veale Wasbrough Vizards

Privacy notices

- A privacy notice should set out the following in plain English:
  - The identity of the data controller
  - What personal data is collected
  - What the personal data is used for
  - Who it is shared with
- Applies to staff, customers, members of the public etc
- A general privacy notice should be displayed prominently, eg on the organisation's website, in the employment manual etc
- Specific privacy notices, eg on application forms
- The obligation is to inform, not get consent

Veale Wasbrough Vizards

Data controllers vs data processors

- Data Controllers: “determine the purposes for which and the manner in which any personal data are processed”.
- Data Processors: “any person (other than an employee of the data controller) who processes the data on behalf of the data controller”.
- Data Controllers liable for the acts and omissions of their data processors.

Veale Wasbrough Vizards

Q2 Data processor or data controller?

- A print company sending out marketing mailshots on behalf of its customer, ABC Ltd

- Is the print company a:

  1. Data Processor?
  2. Data Controller?

Veale Wasbrough Vizards

Q3 Data processor or data controller?

- A law firm processing personal data in connection with advising a client on a family dispute

- Is the law firm a:

  1. Data Processor?
  2. Data Controller?

Veale Wasbrough Vizards

Q4 Data processor or data controller?

- An internet search engine
- Is the search engine a:
  1. Data Processor?
  2. Data Controller?

Veale Wasbrough Vizards

Q5 Data processor or data controller?

- A graphic design company designing a prospectus for a University
- Is the graphic design company a:
  1. Data Processor?
  2. Data Controller?

Veale Wasbrough Vizards

Compliance issues

- Data Controllers must ensure that any processing is carried out under a written contract which requires the DP to provide sufficient guarantees in respect of technical and organisational security measures.
- The contract must also provide that the DP must only act on instructions from the DC.
- The DC has an on going obligation to ensure that the DPs have adequate security in place.

Veale Wasbrough Vizards

Part 2: Security and DPA breaches

Veale Wasbrough Vizards

Consequences of breach: General

- Consequences of breaching the DPA include:
  - Fines of up to £500,000
  - Having to pay compensation to affected individuals
  - Enforcement notices
  - Undertakings
  - Wasted management time
  - Reputational damage

Veale Wasbrough Vizards

The seventh DPA principle

- The vast majority of fines relate to breaches of the seventh principle. Organisations must have appropriate technical and organisational measures in place to prevent misuse of personal data
- The Information Commissioner may also take account of the following when deciding what enforcement action to take:
  - How sensitive the data is and the number of people involved
  - What steps the organisation took to mitigate (and did it self report to the ICO)
  - Whether it was a “one off” mistake

Veale Wasbrough Vizards

Information security breach example

- ABC Charity provides confidential support to victims of domestic abuse. They are in the process of upgrading their ICT and contract with XZY Contractors for the secure destruction of ABC Charity's current hard drives.
- Three months later it comes to the attention of ABC Charity that the hard drives are available for sale on an online auction website.

Veale Wasbrough Vizards

Q6 Information security breach example

If you were the ICO what action would you take?

1. No action
2. Serve an enforcement notice requiring ABC to improve its DPA compliance
3. £50K fine
4. £150K fine
5. £350K fine

Veale Wasbrough Vizards

Examples of circumstances which have given rise to fines

- Personal data stolen after website hacked
- Moving premises and leaving confidential documents behind
- Laptops and other devices being stolen or left on trains etc
- Sending confidential documents to the wrong fax recipient
- Not disposing of confidential documents securely (left in skip outside a supermarket)
- Confusing one customer with another
- Leaving confidential documents on a doorstep
- Allowing staff to work from home without homeworking data protection policies and training

Veale Wasbrough Vizards

Helping to ensure that staff keep data secure

- Technical measures:
  - Passwords (not recommended!)
  - Encryption
  - Mobile device management
  - Remote access
- Organisational measures:
  - Audits
  - Training
  - Policies and procedures

Veale Wasbrough Vizards

Consequences of breach: Personal liability

- Individuals can be personally liable and some breaches amount to a criminal offence
- Stealing Personal Data and accessing without permission is an offence
- Acts committed with the “consent, connivance or neglect” of senior individuals

Veale Wasbrough Vizards

Part 3: Subject Access Requests (SARs)

Veale Wasbrough Vizards

Subject access requests (SAR)

- Individuals have a right to be given a copy of the information which an organisation holds about them
- All of the following are potentially disclosable:
  - Any information held on computer;
  - Photographs, sound recordings;
  - Video recordings including CCTV;
  - Paper records if held in a sufficiently structured filing system
  - Top tip – temp test

Veale Wasbrough Vizards

Subject access requests and tactics

- Individuals will often make a subject access request as part of a complaint
- They will sometimes use subject access requests to try and find fault in how the organisation has approached a particular issue
- Can complain to the Information Commissioner – it costs nothing

Veale Wasbrough Vizards

Q7 Is this disclosable?

Dear Finance Director

I can't believe that Mr Smith is requesting his personnel file! As you know, I can't stand the guy and this does nothing to improve my opinion of him.

He's getting nothing!

1. Disclosable?
2. Not disclosable?

Veale Wasbrough Vizards

Subject access – what staff should be told

- The organisation must comply with the request subject to a number of exemptions
- A request must be in writing but does not have to follow any particular format. No obligation to mention “data protection” or “subject access request”
- Anything that is put in an email is potentially disclosable – no exemption for “embarrassing” emails

Veale Wasbrough Vizards

Managing the request

- How to approach the request:
  - Try and “scope” it, eg ask for more information;
  - Carry out searches to identify the information which is potentially disclosable;
  - Review the information and redact / withhold as appropriate

Veale Wasbrough Vizards

Subject access – exemptions and exceptions from disclosure

1. The information does not fall within the definition of “personal data”
2. Communications with solicitors – but remember litigation disclosure
3. Third party data (other people)
4. No exemption for inappropriate comments made by staff

Veale Wasbrough Vizards

Part 4: Sharing and managing information

Veale Wasbrough Vizards

Request for information from the Police

- Disclosing information to the Police is potentially a breach of the DPA
- For the disclosure to be DPA compliant, the Police must satisfy the organisation that the disclosure is necessary for the prevention or detection of crime or the apprehension or prosecution of offenders and failing to disclose would be likely to prejudice these matters
- The Police can always obtain a court order so if in doubt don't disclose and wait for a court order. However, most organisations wish to co-operate and ensure the DPA requirements are met

Veale Wasbrough Vizards

References

- References given in confidence are exempt from disclosure. This includes references given for the purposes of "education, training or employment, or prospective education, training or employment"
- However, references received are potentially disclosable. This is the case even if the reference is marked "confidential"
- Collaborate and balance rights

Veale Wasbrough Vizards

Monitoring (including CCTV)

- CCTV should only be used with the appropriate notifications
- Overt monitoring eg emails and phone calls is usually permissible subject to:
  - Impact assessments
  - Fair processing notices should be included in the data protection policies and procedures
- Covert monitoring – should only be used for investigating criminal allegations or equivalent malpractice
- ICO registration

Veale Wasbrough Vizards

Policies and procedures

- For staff:
  - **Overarching data protection policy**
  - **Remote working and bring you own device to work policy**
  - **ICT acceptable use policy**
  - Privacy notice
  - Document retention policy (should cover staff, financial, health and safety, legal etc)
  - Website provision of information (cookies, privacy, disclosure regulations etc)
  - Data protection compliance checklist

Veale Wasbrough Vizards

Audits

- Carry out audits at regular intervals and also whenever personal data is used in a new way or when problems are identified (eg, a new IT system, new office or factory)
- The questions which should be asked as part of an audit include:
  - What arrangements are in place when staff work from home (eg, encryption, remote login etc)
  - Arrangements for security
  - Staff data protection training

Veale Wasbrough Vizards

Helping to ensure compliance

Organisational measures

- Having policies and procedures:
  - Keep them up to date and ensure that staff have read them and know where to find them
- Training:
  - For new staff
  - Best practice refresher training every 2 to 3 years
  - On-going audits and risk assessments

Technical measures

- Encryption, mobile device management and remote access
- Limit access to “need to know”

Veale Wasbrough Vizards

Part 4: Any questions?

Andrew Gallie
Senior Associate
agallie@vwv.co.uk
0117 314 5623

Veale Wasbrough Vizards

www.vwv.co.uk | Offices in London, Bristol & Birmingham
Lawyers & Parliamentary Agents