Data Protection and the GDPR

Training for Councillors

Kevin Toogood and Jane Mars, Legal Services

Introduction

- General Data Protection Regulation (GDPR) in force 25 May 2018 and Data Protection Act 2018
- DPA 1998 revoked – a new regime
- Tighter regulation & higher penalties by the Information Commissioner's Office (ICO)
- Individuals more aware of their information rights. We had 708 FOI/Subject Access Requests in 2016 and 750 in 2017. Most organisations seeing a year on year increase in numbers of requests made. Expect claims to rise.
- TMBC review of processes and training

Why is this important?

- Trust – putting residents first
- Value of personal data in a virtual world
- Data Protection breaches can carry significant risks to the Authority and individual Members:
  - Financial Risk
  - Reputational Harm/ Harm to residents
  - Legal Risk
- ICO stated in August 2017:

  "Local authorities handle lots of personal information, much of which is sensitive. If that information isn't kept secure it can have distressing consequences.

  It is vital that **all** council staff take data protection seriously"

Examples of Enforcement Action by the ICO

- Information Notices, Directions, Voluntary and Enforced Audits & Assessments (Medway – training)
- Stop Notices – can effectively close any registered business
- Financial penalties. Up to 4% turnover/20 Million euros – some recent examples:
  - £325k May 2018 CPS – loss of unencrypted DVDs
  - £120k March 2018 Kensington & Chelsea – revealing homeowner IDs in response to an FOI enquiry
  - £100k Aug 2016 Hampshire County Council – insecure disposal of data
- Personal liability – ICO can impose penalties on individuals acting outside their professional remit. You must only request access to information on a need to know basis, not on an access all areas basis – Recent action against NHS staff member who accessed and disclosed personal data to friends. Job loss, prosecution, fine and costs.

What is involved?

Data Protection seeks to protect the information rights of individuals by controlling the processing of:

- Personal Data; and
- Special Category Personal Data/Criminal Convictions

In essence, it governs how and why we collect information, how we store it, share it and dispose of it.

- Privacy by Design
- Privacy Impact Assessments will be mandatory for some processes
- Information Asset Register – Corporate record keeping to show what information held where and for what purposes

What is Personal Data?

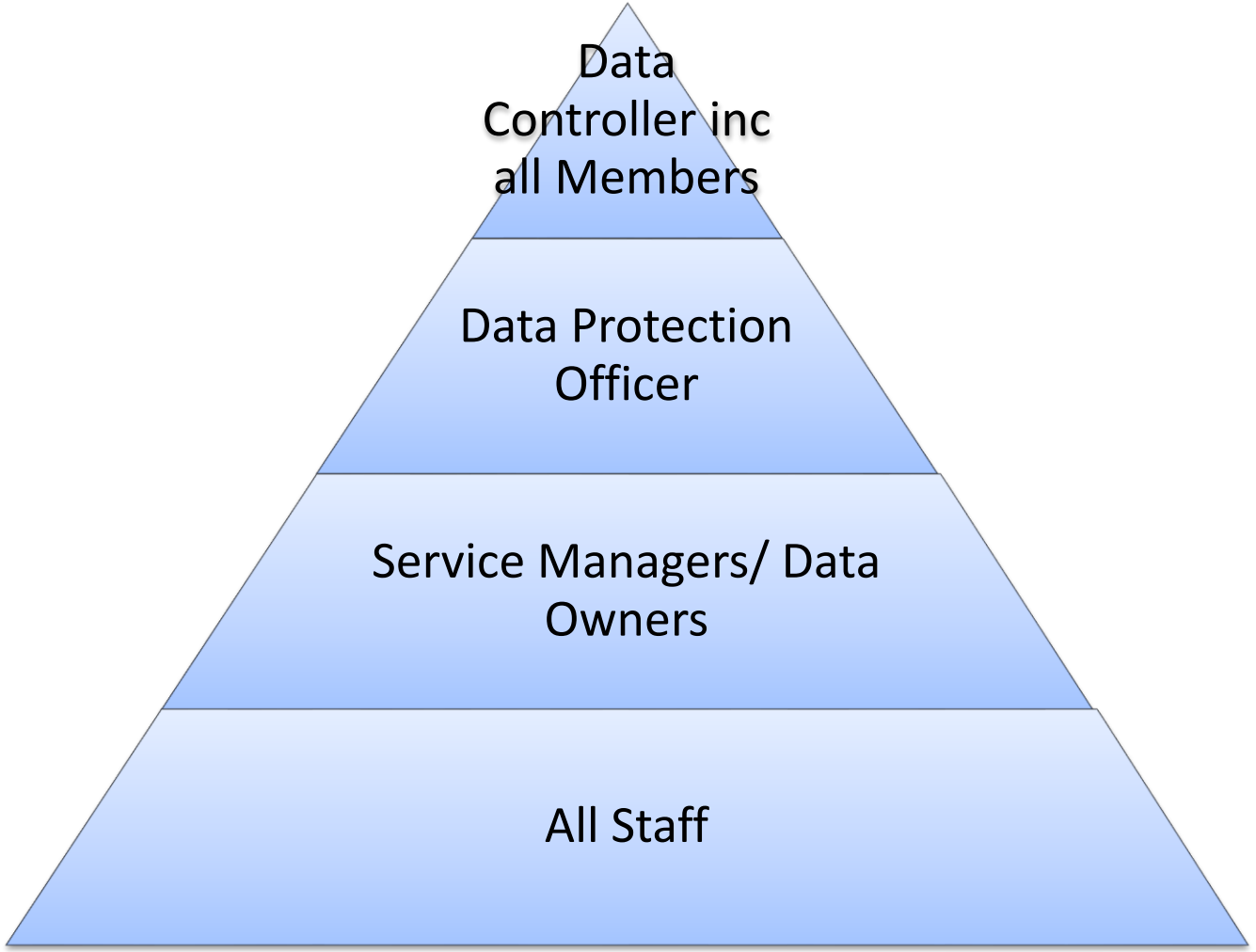
- *"personal data"* means data which relate to a living individual who can be identified—

  (a) from those data, or

  (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual;

Control of Data at TMBC



Control of Data at TMBC (2)

- Data Protection Officer (DPO) responsible for corporate compliance- e.g. ensuring policies fit for purpose etc.
- DPO chair of Information Governance Group (IGG)
- IGG considers instances of DPA/ GDPR breach and whether these should be referred to ICO
- Members are also Data Controllers in their own right

The Data Protection Principles

Fair and lawful, open and transparent
Collected for a specified purpose
Necessary and not excessive for its purpose
Accurate and kept up-to-date
Not stored any longer than necessary
Kept safe and secure

Processing Personal Data (1)

- The “lawful basis” of processing:
  - Consent to processing;
  - Necessary in accordance with a contract with the data subject or at their request with a view to entering into a contract;
  - Necessary for compliance with a legal obligation;
  - Necessary to protect the vital interests of the data subject;
  - Necessary for performance of a public task carried out in the public interest (NB in particular s.8 DPA ’18 - *activity supporting or promoting democratic engagement*);
  - Necessary in the pursuit of legitimate interests (except where causing prejudice to rights and freedoms of data subject);

Processing Personal Data (2)

- At the point of collection. Think:
  - do you *need* it?
  - Lawful reason?
  - explicit consent freely given (and knowingly given)
- Using the data:
  - what is processing?
  - proper lawful purpose?
  - why did you collect it?
  - did you explain the potential use(s)?
  - Privacy Notices/ auto-reply/ footer

Processing Personal Data (3)

- Sharing the data:
  - can you?
  - FoI/EIR
  - identify *and record* reasons
  - Privacy Notice
- Review:
  - should you be keeping it?
  - for how long?
  - is it still accurate?
- Disposal and the “right to be forgotten”

Special Category Data

- Sub category of PD to which additional conditions for processing apply. SCD is:
  - personal data consisting of information as to—

    (a) the racial or ethnic origin of the data subject,

    (b) his political opinions,

    (c) his religious beliefs or other beliefs of a similar nature,

    (d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),

    (e) his physical or mental health or condition,

    (f) his sexual life,

    (g) Genetic data

    (h) Biometric data (e.g. fingerprint)

Processing Special Category Personal Data

- At least one of the standard conditions *and* at least one of the following must apply:
  - Explicit consent to processing;
  - Necessary under law in connection with employment, social security or social protection law;
  - Necessary to protect vital interests of data subject or another person where consent cannot be obtained from data subject (or where consent withheld by data subject in order to protect vital interests of another);
  - Activity of not for profit political, philosophical or religious body in relation to its members with appropriate safeguards in place;
  - Has been made public, deliberately, by the data subject;
  - Necessary for legal proceedings (or prospective proceedings), legal advice or otherwise establishing, exercising or defending legal rights;
  - Necessary in the **substantial public interest** (NB: in particular Sch 1 Pt 2 DPA '18 - *elected representatives responding to an individual's request*);
  - Anti-fraud activities by anti-fraud organisations;
  - Disclosures in good faith under terrorism or proceeds of crime legislation;
  - Necessary for medical purposes;
  - Necessary in the interest of public health
  - Necessary for archiving in the public interest, scientific or historical research or statistical purposes

Example (SCD)

- Mrs Smith is an elderly resident of Tonbridge with physical disabilities
- She has been attempting to obtain a Disabled Facilities Grant from the Council and is seeking your help
- Are there any particular Data Protection issues with the information you would need to share with Housing Officers?
- Is there a legal basis for you to share it (without first obtaining her consent to do so?)

Criminal Conviction Data

- Further sub-category of PD with special conditions required for processing. Requires an Article 6 lawful basis (as above) plus:
- An authorisation “under Member State law” (i.e. the DPA ’18 in UK law). “Necessary” in connection with:
  - Employment/ social security/ social protection law
  - Health & social care
  - Public health
  - Research (scientific, historical, statistical)
  - Statutory purpose
  - Administration of justice
  - Prevent/ detect unlawful act
  - Protecting public from dishonesty
  - Preventing fraud
  - Preventing terrorist financing/ money laundering
  - Support for disabled/ medically infirm
  - Safeguarding
  - Elected representative responding to an individual’s request
  - Consent
  - Information is in the public domain
  - In connection with legal claims

Handling Casework (1)

- Residents can expect you to raise issues with the Council on their behalf. Can you share their details with staff?
- Yes – within limits
    - Is it *necessary* for carrying out a public function or promoting democratic engagement?
    - Special Category Data processing permissible where *necessary* for an elected representative to take action on behalf of an individual
    - Only forward to others e.g. to relevant ward colleague/ MP if they *need* to act on it
  - BUT
    - Don't otherwise "CC/ BCC" ward colleagues/ MP/other parties ("for information") without express consent – ask don't assume.

Handling Casework (2)

- Where is the information stored?
  - TMBC inbox or Mod.gov “private” papers viewed on TMBC tablet (secure by design, technical and organisational measures in place, policies in place, capable of ICO audit)
  - “Cloud” email or document server? (Gmail, Ymail, dropbox) (risks of hack/ compromised accounts, transfer out of jurisdiction)
  - Could you prove to the ICO that the PD/ SPD you hold on your own equipment is secure?
  - Could you prove your personal e-mail account is secure?

Getting it Right

- **Members are personally responsible for personal data they hold;**
- Ask residents seeking your assistance if they are happy with you sharing their details (e.g. with MP, ward colleagues, council staff) and explain why (NB you may be ok doing so without express consent but it is a good practice to get into, as it covers wider sharing that might not be seen as “necessary” under the legislation;
- When obtaining personal data, make sure it is done in private, take no more than is necessary, get explicit consent, write down no opinions, date your notes, beware data creep, safe storage at home in locked cabinets, no information left on desks/kitchen tables/in cars etc, sharing & data sharing agreements, retention policies, disposal, shredding, use a privacy notice in your email. Get into the habit of bringing any old papers/ disks/ memory sticks into TMBC offices for secure disposal
- Read policies, engage in training – more below

Getting it wrong

- Technical and structural measures – IT security/ hacking issues /physical security measures – secured doors, cabinets, clear desk policy in home offices- who else has access?
- Self reporting to ICO – consult the DPO/ DDPOs but it is your responsibility
- 90% + issues arise from human error:
  - Accidentally sending info to wrong recipient eg drop down email addresses/ phone calls
  - Disclosure in conversation
  - Data loss or theft – documents on bus, laptops in taxis etc
  - Don't allow laptops/ papers/files to be read from behind etc. Read policies. Is the laptop password protected?
  - Review storage of hard copy data, dispose of paperwork securely

Training and Review

- All members to be offered DPA training (this session)- and as part of member induction post- elections;
- Online training available – check with HR if not registered for e-learning already;
- Refresher training every two years for all;
- Think - What do I need to look at/change?

Contacts

- Data Protection Officer: Adrian Stanfield
- Deputy Data Protection Officers:
  - Lynn Francis
  - Kevin Toogood
- Legal Service for general advice (Lynn, Kevin, Jane Mars, Simon Jones)