General Data Protection Regulation (GDPR)

Emma Pheby

Introduction

- Emma Pheby

- Background to new legislation – increasing amounts of personal data supplied to organisations; far more online processing; increased risk of identity fraud – epidemic levels (500+ cases a day in UK) – accessing bank a/c, purchase cars, loans etc

GDPR Readiness

- In 2017: ICO Survey revealed:

26% LA had not appointed a DPO;

60% LA had not appointed an information governance manager

59% LA had no assigned Information Asset Owners

59% LA didn’t undertake Privacy Impact Assessments (good practice DPA98 & mandatory under GDPR for ‘high risk processing)

31% LA didn’t have mandatory data protection training for employees who process personal data

- Today is an interactive session – 5 minutes to discuss with neighbours - Where is your LA in GDPR planning? Not started? Just started? Well prepared but some issues of concerns? Fully prepared and reviewing? Where are your problem areas?

GDPR Overview

- EU Legislation – directly implemented 25/05/2018
- Data Protection Bill 2018 (process of Royal Assent – proposed 15/5) – Enacts GDPR (post-Brexit clarity) & Derogations from GDPR
- Fines levied - £500k  € 20M
- Other enforcement action (eg limit processing)
- **Increased obligations on organisations; increased rights data subjects; increased powers & fines by regulator**
- Practical presentation & available afterwards for any questions

Definitions under GDPR

- **Personal Data**: Personal data is information which identifies a living individual directly or indirectly, or from which an individual is identifiable.

In short, it is **not just about identifying a person by name but also about identifying a single person whose name is not known**. Indirect identification could occur through different data combinations. Online identifiers and location identifiers are additionally referenced in the GDPR.

- **Special categories of personal data – Article 9 –** racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, processing genetic data, biometric data, health or data concerning sex life/sexual orientation – extra safeguards (see A9(2)(b) – including can process where it is for the purposes of '***social security*** or social protection law'…

- **Data Subject**: The individual who is identified/identifiable from the personal data.

- **Processing**: can include collecting, recording, storing, adapting, altering, retrieving, consulting, using, disclosing, disseminating, restricting, erasing or destroying personal data.

- **Data Controller**: the public authority, individual (or other organisation, body or agency) who determines the purpose and means of processing the data.

- **Data Processor**: the organisation who process personal data for the Controller.

For example: Where a local council use an archiving service who will store and review/retrieve requested files, the council will be the Controller and the archiving service will be the Processor.

Complying with Article 5 – Six Principles of processing –Data Retention

- A5(1)(e) – personal data should be 'kept in a form which permits identification of the data subjects for **no longer than is necessary** for the purposes for which the personal data are processed'
- Determining how long is '*necessary*'
- RETENTION GUIDELINES – reflective of the records your organisation holds? Up to date?
- How decide? Subject specific primary/secondary legislation, good practice, business need – justification/consideration
- Legislation – Limitation Act 1980 (how long bring contractual claim etc); Specific legislation eg Audit Commission Act 1998; Taxes Management Act 1970
- Once RETENTION length decided – how can this be applied? Data cleansing ability? Paper files?
- **Steps: Update Retention Guidelines & apply!!!**

Other Article 5 principles

- A5(1)(a) – Personal data shall be processed '**lawfully**, **fairly** and in a **transparent** manner' – will revisit lawfully – fairly and transparency = use of clear unambiguous language, openness – will look at this in Privacy Notices. *Note – When considering e-billing ensure that we are transparent about the collection of emails for this purpose (consider other legislation eg Equality Act)*
- A5(1)(b) – Personal data shall be '**collected for specified**, **explicit** and **legitimate** purposes and not further processed in a manner that is incompatible with those purposes' – Why are you collecting the data? Are you only using it for those purposes (there are exceptions eg fraud/prevention of crime)? Are you clear and transparent to data subjects? - can't just give it to marketing; use for systems testing
- A5(1)(c) – Personal data shall be '**adequate**, **relevant** & **limited** to what is necessary' – Do you need all the personal data you are collecting? IE do you use it all & make it clear why you collect it all
- A5(1)(d) – '**accurate**, and, where necessary, kept **up to date**' – **how do you update data?**
- A5(1)(f) – 'appropriate **security**' – who has access to the personal data? Is it securely locked away? Password protected? Encrypted? IT security measures (firewall)? Security during transportation/transmission?

Accountability

- Last Article 5 principle..
- Accountability:

1. Policies (Data Protection, Privacy Policy, Records Management Policy, Retention Guidelines, Home & Remote Working Policy, data Sharing Agreements etc) – Reviewed, easily accessible, applied?
2. Training – mandatory & refresher – e-learning? record of attendance
3. Team specific Guidance – addressing/managing identified risks eg Security checks you undertake to identify a customer; consent & process of dealing with third parties; risk limitation steps taken; relevant policies & raising awareness of these; breach notification; data protection champions (how they cascade information back)
4. Not enough to apply GDPR – need to show you are compliant and to have clear and systematic processes not ad hoc processes

Steps: review/draft relevant policy; review data protection training – mandatory/refresher/recording of attendees; create team specific guidance of procedures

Lawful processing ground

- There are 6 grounds for lawful processing, however only 5 of these are ordinarily available to public authorities. Rarely, by consent.
- ICO Guidance identifies that most of a local authorities processing will be carried out under the following lawful processing ground:
- A6(1)(e) – ‘processing is necessary for the performance of a task carried out in the public interest or in the **exercise of the official authority** vested in the controller’.
- **Steps: identify ground. Data subjects rights depend on lawful processing ground used. This will need to be detailed on your A30 Record of processing.**

Variation of Contracts with data processors

- Step One – Understand who is a data processor
- Step Two - identify relevant contracts (Contracts register and elsewhere) which continue post-25/05/2018 Contract examples – bailiffs? Systems providers? Mail service providers?
- Step Three – Draft revised terms & conditions to include the mandatory requirements set out at Article 28(3)
- Step Four – Ensure new contracts include these terms & conditions
- Step Five – Vary relevant contracts which will run post-GDPR

Steps overview: Review all contracts with processers; vary standard T&Cs

Privacy Notices/Fair Processing Notices

- Article 13 details information required to '**be provided where personal data collected from the data subject**'
- Revise Privacy Notices – online & forms to include this information
- Details to include:

✓ Identity/contact details of the Controller & where applicable controller's representative);
✓ contact details of the DPO;
✓ processing purpose & legal basis for processing;
✓ recipients' of the data;
✓ (transfer of data to a third country);
✓ retention/criteria for retention;
✓ Data subjects rights & right to lodge a complaint with ICO
✓ Where processing under lawful ground of consent – right to withdraw consent at any time
✓ Whether the provision of personal data is a statutory/contractual requirement – & possible consequences of failure to provide this data
✓ (details of any profiling ie automated decision making)

- **Clear plain English & accessible to the relevant customers – headings can be useful for clarity -ICO advise provide layered info.**
- If further processing for a different purpose – Data subject must be provided with relevant information
- **Steps – review all privacy notices & update as required**

Data Sharing

- **Internal** → Who? Why? Fair, transparent & lawful?

Example 1 – **Marketing** – should be by consent – when privacy notice provided about why details being taken by Revs Bens should also have clear separate wording about marketing with opt-in consent only

Marketing = promoting aims as well as selling goods/services directed at particular individual/s

In these circumstances marketing dep. can have those details of individuals who have clearly consented to marketing

Example 2 – **Grants' team; housing team; benefits team** – should be stated in the privacy notices that you intend to share this data with other services within the Council – to ensure lawful, fair & transparent. Data sharing policy?

- **External** → Who? Why? Fair, transparent & Lawful? Data sharing policy?

Example 1 – Data to Company who reviews Single Person Discount data –fair, lawful & transparent (data sharing agreement? Privacy notice details?)

Note– GDPR (as DPA98) makes exceptions to the details where it is for the 'assessment or collection of a tax or duty or an imposition of a similar nature, to the extent that the application of those provisions would be likely to prejudice any matter' – so consider whether to inform or whether if individuals were informed if it would prevent collection of taxes.

Steps – Review data sharing agreements; review/create data sharing policy

Breaches

- New requirement -DPO to report relevant breaches to ICO without undue delay/within 72 hours; take mitigating steps (contacting parties involved; prevent future similar incidents – procedural changes – Record changes (accountability)
- Fine for non-compliance
- Fines – huge increase – also reputational risk & risk of other enforcement action
- System in place to identify breaches & to report promptly?
- Speak to team about notification immediately – discuss process
- Identify risks – take steps to reduce risks!
- Steps: Breach Notification Policy?; Risks identified within team & mitigating steps taken & recorded?

Data Subjects Rights

- Increased 6 rights – portability, erasure, rectification, access (SAR), objection and restrictions
- Not absolute rights
- Depends on lawful processing ground
- So for Revs & Bens where lawful processing ground A6(1)(e) –public ground erasure & portability do not apply, objection does apply
- Any of these rights exercised should be overseen/recorded by DPO
- 1 month time limit

Other Issues to consider

- DPO – role

Has a DPO been assigned? Role includes – compliance; liaison with regulator; DPIA; breaches, A30 Record, data subjects rights

- A30 Record of Processing

Have you created a record of processing? Required maybe requested by ICO. Overview of personal data processed across whole organisation.

- SIRO; Information Asset Owners; Data Champions

Other corporate issues to consider

- Technical & security measures review – locked draws? Limited access?
- IT – back-up review; security measures for IT & process for dealing with breaches
- Emails – 46% increase in breaches by email (ICO) – mitigation steps? Autosuggest removal? Auto-delay? Attachments password? Secure emailing where possible
- Policy reviews – Data Sharing Policy, Data Protection Policy, Privacy Policy, Breach Notification Policy/Procedure, DPIA Policy, remote/home working policy

Questions