GDPR: ARE YOU READY?

Iain Malloch. Data Privacy Officer

Halifax Intermediaries and BM Solutions, Scottish Widows Bank

MYTH OR TRUTH?

LLOYDS BANKING GROUP

- Replaces the Data Privacy Act 1998
- Europe-wide, despite Brexit!
- Comes into force 25th May 2018
- Keeps companies honest and protects the population at large
- Gives people more control over how their data is used , trust in data security can bring commercial advantage
- Applies to data controllers and data processors
- Brings clarity on consent
- Redefines what is personal data
- Fine structure changes
- Incremental build on current DPA

WHAT IS PERSONAL DATA?

LLOYDS BANKING GROUP

'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'

Data categories and examples

Contact data e.g. home address	**Technical data e.g. IP addresses**	**Special categories e.g. health data**	**Documentary data e.g. ID&V evidence docs**
Financial data e.g. income	**Locational data e.g. mobile device location**	**Behavioural data e.g. spending patterns**	**Communications data e.g. emails**
Social relationships data e.g. spouse	**Open data and public records e.g. bankruptcies**	**Transactional data e.g. payments made**	**Photograph**
Usage data e.g. credit use	**Contractual data e.g. products held**	**Socio-demographic data e.g. occupation**	**Consents e.g. service preferences**

Without data your business cannot function

WHAT IS PROCESSING ?

‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction’

Each and every one of you process large amounts of data every day

ARE YOU READY?

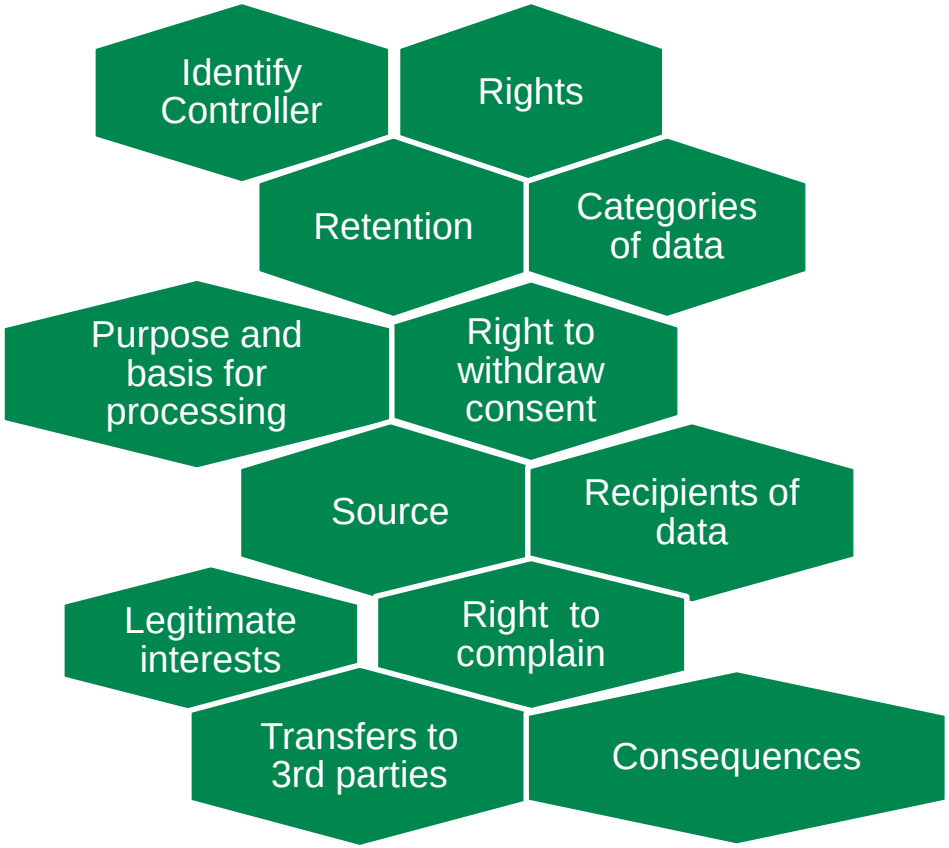
AWARENESS

- Who in your organisation needs to know about this ?
- Knowledge
- Resource implications?
- Timing
- Are you DPA compliant?
- Start to identify potential problem areas
- Plan

WHAT INFORMATION DO YOU HOLD?

- Ties to GDPR accountability principle
- Where is your data held
- What types of data do you hold/process
- Do you send data to others to process
- Is your data up to date/accurate
- Where did it come from

TELL - PRIVACY NOTICES



INDIVIDUAL RIGHTS

- To be informed
- Of access
- To rectification
- Erasure
- Restrict processing
- Data portability
- Object
- Not to be subject to automated decision making or profiling

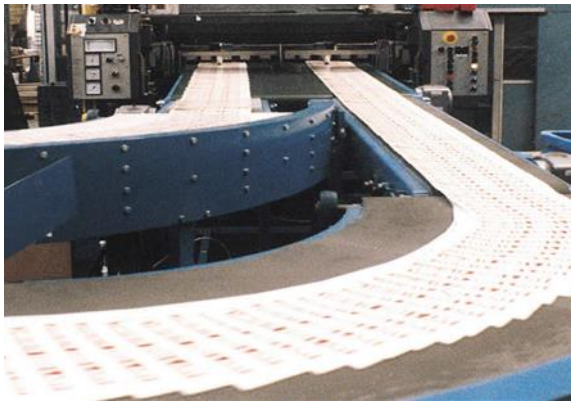
SUBJECT ACCESS REQUESTS .
ON WHAT BASIS ARE YOU PROCESSING?

Subject Access Requests

- No charge under GDPR
- One month to comply
- Can refuse

Processing

- On what basis are you processing ?
- Document it
- Have you told them (DPN)
- You will need to advise on a DSAR



CONSENT

This will continue under GDPR, however, the threshold for a valid consent will be significantly raised as customers must take positive action to give their consent. Pre-ticked boxes are not allowed, silence will be treated as not having given consent. Consent must be as easy to withdraw as it is to give.

Giving Consents	Managing Consents	Audit of Consents	Historical Consents	Consent of Minors
➢ explicit ➢ Unambiguous ➢ fully informed ➢ freely given	➢ Must be able to evidence and manage consents over time ➢ Stop processing personal data where that processing is reliant upon consent and such consent is withdrawn.	Must be able to provide evidence of how and when a data subject provided consent and what the consent was for.	If consent has previously been provided, must demonstrate that the data subject has provided a freely given, specific, informed and unambiguous indication of their wishes, and when and how that consent was given	➢ Ensure that when processing the data of a child below the age of 16, consent has been given by a parent or guardian ➢ make every effort to verify that consent is given or authorised by the parent or guardian.

DATA BREACHES

- Potential notification to the ICO
- Potential notification to the client
- Procedures
- Think reputation

DATA PRIVACY BY DESIGN . DATA PROTECTION IMPACT ASSESSMENTS

- Privacy by design becomes ‘express legal requirement’

- DPIA
  - Best practice for change of process/system etc.
  - New technology
  - Who needs to be involved
  - Data processors

DATA PRIVACY OFFICER

- Do you need a Data Privacy Officer?
- Best practice would be at the very least to have someone responsible for your data
- Follow the spirit of the legislation
- Be proactive
- Involve your colleagues
- Communicate

BEST PRACTICE

- Passwords
- Locked cabinets
- Postage
- Files
- Storage
- Data processors
- Laptops
- Data Privacy Notices
- Retention
- Breaches
- DSAR
- Communicate

THANK YOU