GDPR a marketing perspective

My background

25 years in direct and database marketing

Data Compliance Consultant at The Data Compliance Doctors

Co-Founder and Director of ListGenie

Worked in eCRM agency, marketing services and client side roles

Member of the DMA email marketing Council and DMA GDPR and Legal Hub

The core GDPR principles

1. Personal data must be processed in a fair, lawful and transparent manner.
2. Purpose limitation: use personal data only for specified, explicit and legitimate purposes.
3. Data minimisation: only process personal data that is adequate, relevant and limited to what is necessary
4. Accuracy: personal data must be accurate and kept up to date
5. Data retention: personal data should not be kept any longer than is necessary
6. Data security: personal data must be processed in a manner that ensures appropriate security of the data
7. Accountability: Article 5(2) requires that “the controller shall be responsible for, and be able to demonstrate, compliance with the principles.”

Some key considerations for marketers

Data audits – personal data

What?
is it

- Prospect data – potential customers
- Current customer data – existing customers
- Lapsed customer data – former customers
- B2B or B2C

Where?
did it come from

- Transactional data
- Service and care data
- ‘Bought’ in data
- Online data – cookies, behaviour
- Data from profiling – enriched or augmented

How?
Does it leave the business

- Shared with external data processors
- Shared between other group entities
- Stored in non EU countries*
- ‘Sold’ to third parties

Legal basis for processing?

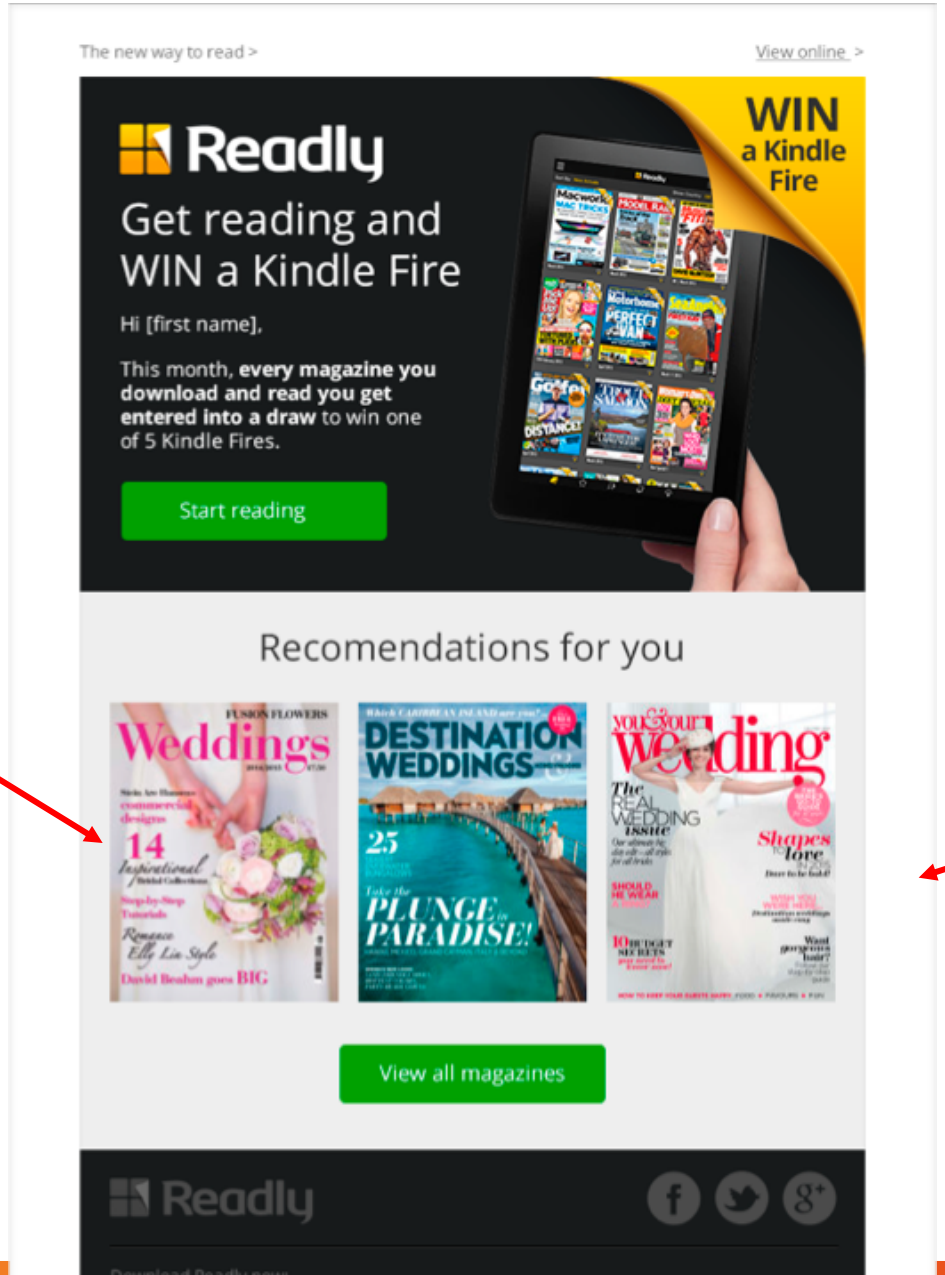
- Contractual necessity: necessary for performance of a contract
- Compliance with legal obligation: employment
- Vital interests: life or death - sharing medical records
- Public interests: taxation, reporting crimes, product safety, election campaigns
- Legitimate interests: covers controller legitimate interest as long as data subjects expectations are met
- Consent: the data subject has consented to the processing

Consent or legitimate interest – Email*

Option 1

Email content is generic. Recommendations are the same for everyone

Marketing consent required only (PECR).

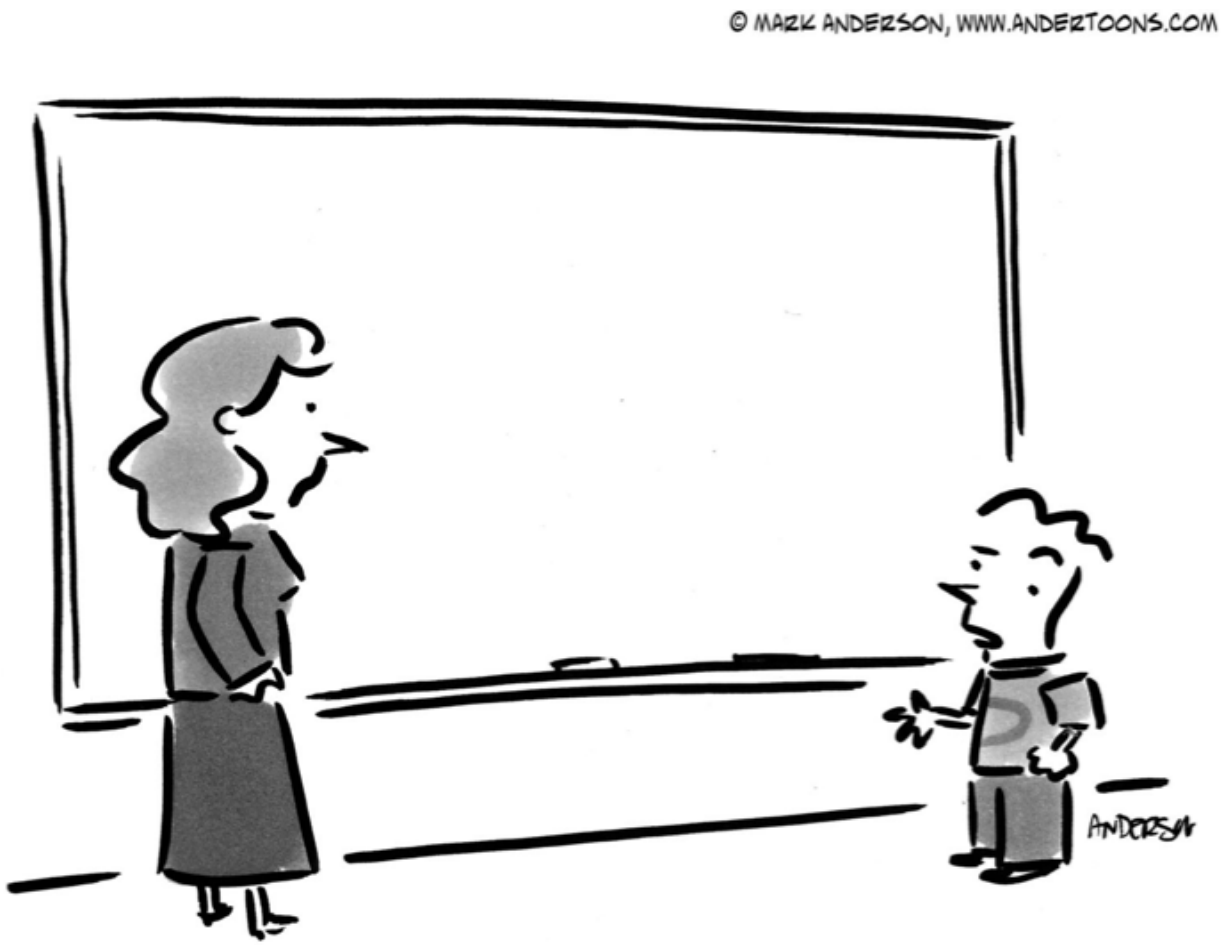


Option 2

Email content is dynamically personalised based on behaviour, interests, and demographics. Recommendations are the same for everyone

Marketing consent required (PECR) and GDPR alignment with consent or legitimate interest to process and profile.

*You need both..



"Before I write my name on the board, I'll need to know how you're planning to use that data."

GDPR: additional demands on informing data subjects

	Purpose of the processing and the legal basis for it	Any recipient or categories of recipients of the personal data	
Identity and contact details of the controller or representative	Use of automated decision making eg profiling and how decisions are made	Details of transfers to third country and safeguards	The right to withdraw consent at any time, where relevant
Retention period or criteria used to determine the retention period	The existence of each of data subject's rights	The right to lodge a complaint with a supervisory authority	The legitimate interests of the controller or 3rd party, if applicable

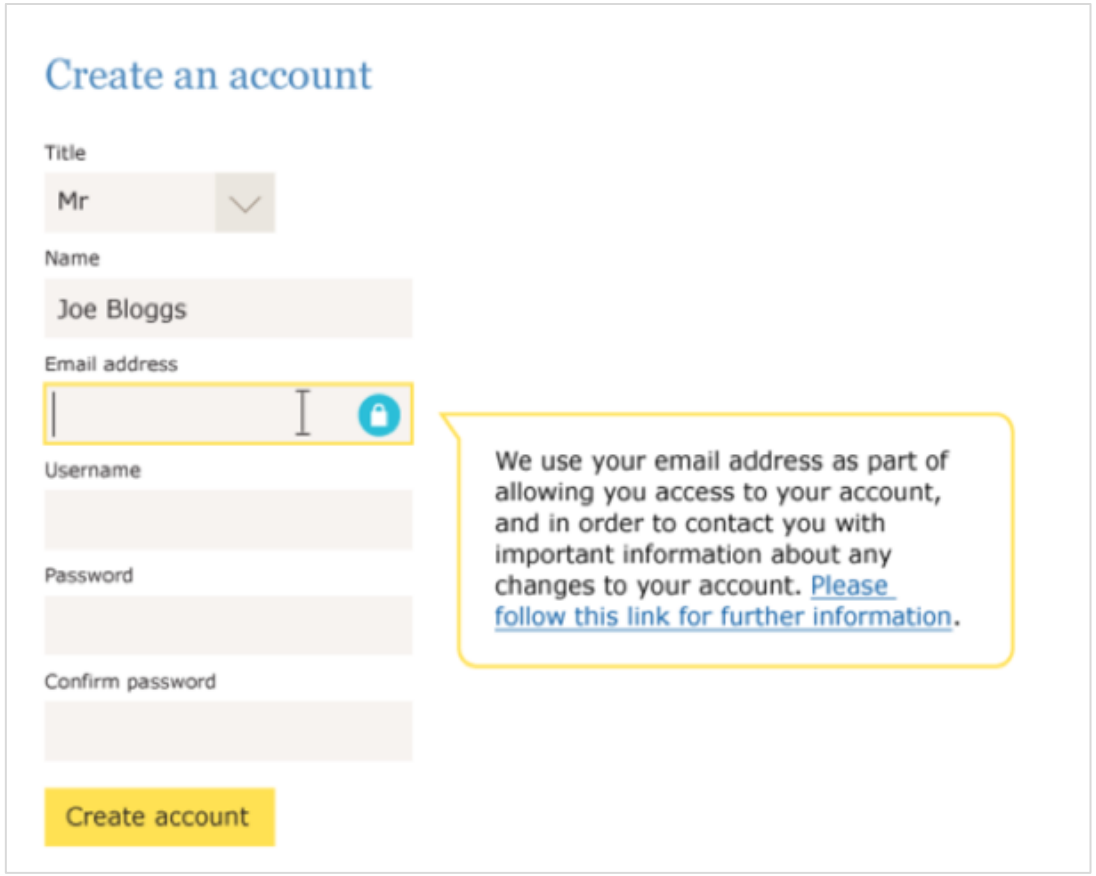
Privacy notice development

A significant amount of additional information needs to be communicated in a notice under GDPR

Consider a layered approach:

- Just-in-time notices
- Video
- Icons and symbols
- Privacy dashboards.

Use plain English!
https://readable.io/text/



Privacy notice - creative and intuitive

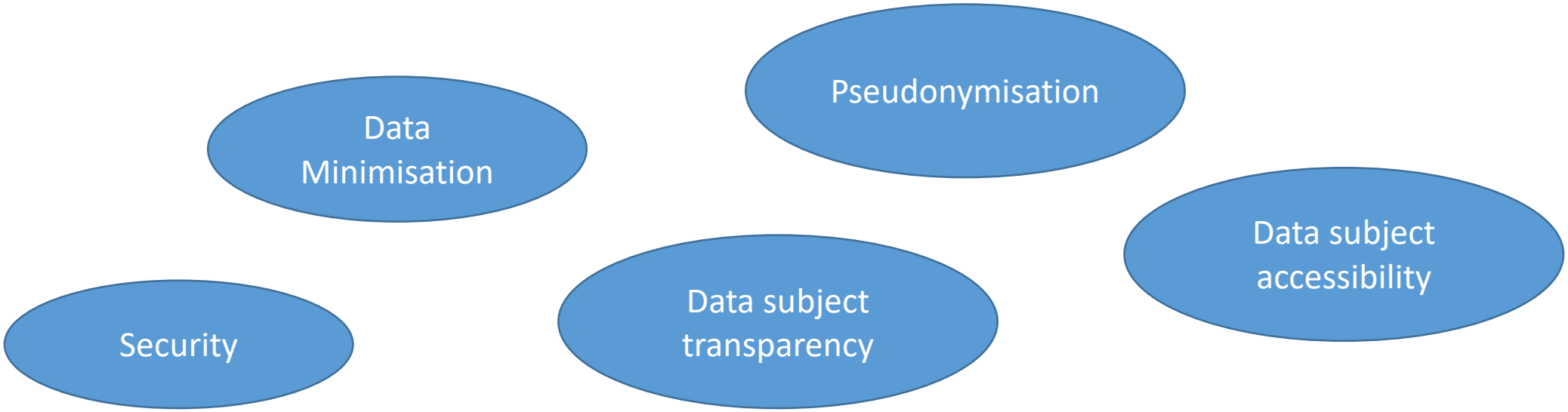
The GDPR states that privacy notices must be:

- concise, transparent, intelligible and easily accessible (even with all information required!)
- written in clear and plain language, particularly if addressed to a child; and
- free of charge

There are many ways to present privacy notices and inform a data subject. They need consideration and planning.

Privacy by Design

Implementation of privacy principles into policies that will govern the development of new projects and the management of existing ones.



Privacy impact assessments

- **Vendor selection** – evaluation of ESP, hosting providers, analytical services, data bureau / fulfilment houses, data services providers
- **Developments** – new websites, databases, tools, mobile apps, portals, product innovation, new product development
- **Processing change** – profiling, behavioural analysis (AI), enrichment, data augmentation, gap analysis

!

Does the proposed processing activity represent a real risk to the rights and freedoms of the data subject?

Example PIA process

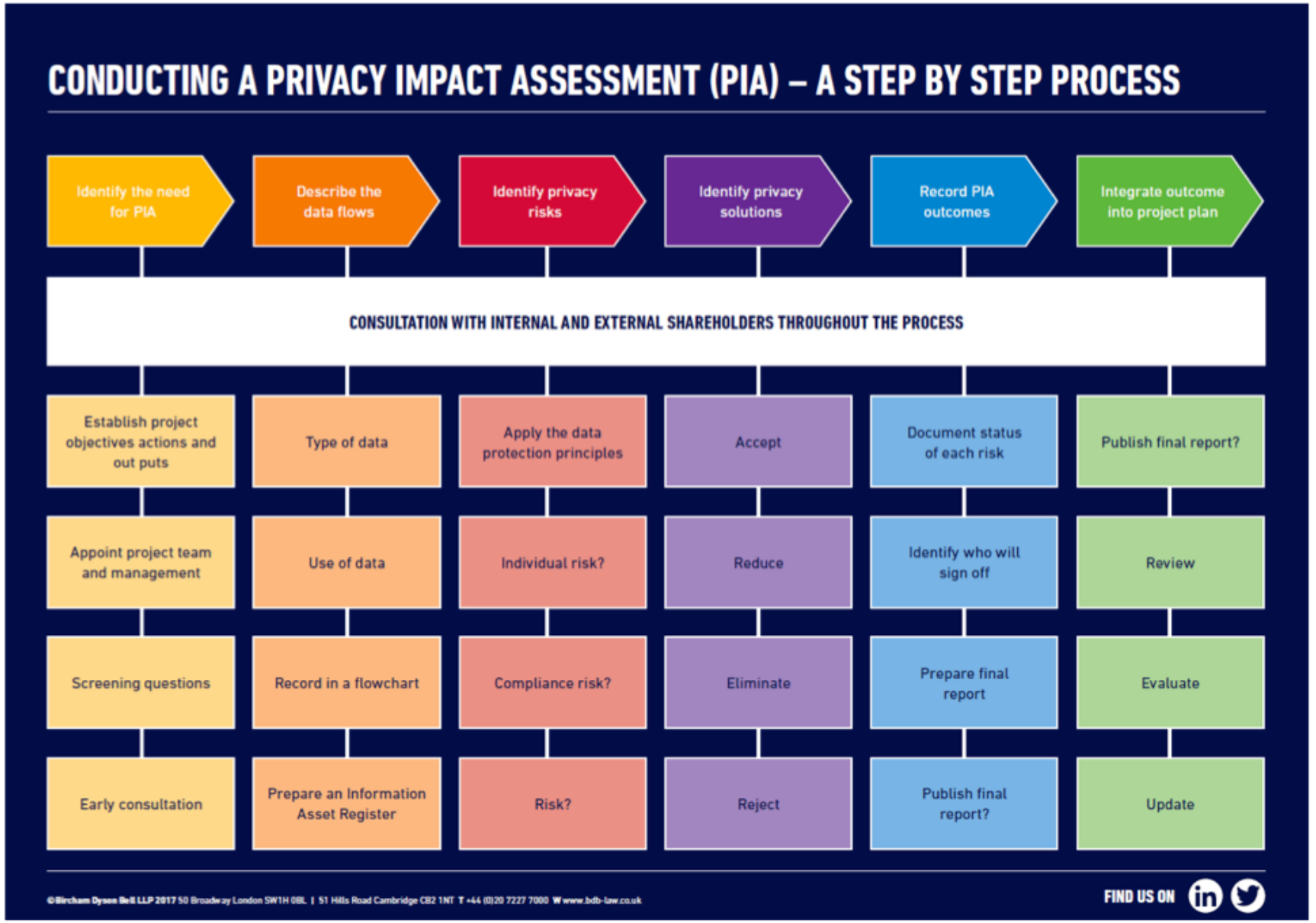


Image: Bircham Dyson Bell July 2017

Subject Access Requests

Data subjects are entitled to:

- Confirmation data is being processed
- Have access to it if so – for free (further copies may be charged for)
- Other supplementary information, such as may included in the privacy notice:
  - *Processing purpose*
  - *Categories of data*
  - *Recipients of data*
  - *Storage duration*
  - *Automated processing detail – profiling logic to be made avilable*
  - *Data transfer to a 3rd country and safeguards*
  - *Where to raise complaints*

The ICO endorses remote access to such information where possible.

! Marketing teams and media owners must resource effectively. Jan 2018 GDPR consumer campaign.

Evidence of compliance

- ✓ Privacy notices – current, clear, transparent and accessible. Log changes.
- ✓ Manage and record consent – mechanism, time, date, preferences
- ✓ Develop robust contracts between data controllers and data processors
- ✓ Security policy
- ✓ SAR process
- ✓ Data audits
- ✓ Document PIA
- ✓ Document a GDPR roadmap

Useful links

Data Compliance Doctors www.thedatacompliancedoctors.co.uk

ListGenie www.listgenie.co.uk

ICO https://ico.org.uk/

DMA https://dma.org.uk/

The Data Protection Network https://www.dpnetwork.org.uk/

Anything else... simon.jeffs@datacompliancedoctors.co.uk

Thankyou!