



Data Sharing Review Secretariat
5.26 Steel House
11 Tothill Street
London SW1H 9LH

11 February 2008

Cc: Christine Andrews

Dear Sirs

I'm pleased to provide our thoughts for the ICO's request for consultation on Data Sharing. For time reasons I have had to be selective on which questions to address but I would be pleased to provide further information after the 15th February if required.

Section 1: Background

DQM Group, a data value management specialist, is **market leader in protecting commercial and marketing data from theft and misuse**. In particular, we provide data tracking and compliance auditing services for most leading data and media owners in the UK. We operate largely in the direct marketing and publishing industries. Over the last 11 years we have identified considerable misuse of data (see attached reports).

We also help our clients develop value and new revenues from data. This can mean us aggregating, enhancing, managing and processing data. This data may include personal information that is typically used in direct marketing.

Our Methods for monitoring and protecting use of commercial and marketing data would be equally effective for all applications of personal data especially to support data sharing in the public sector, which we believe several substantial benefits for 'joined up' Government.

Also, we believe strongly that the direct marketing (DM) industry generally should do more to reduce concerns amongst consumers about how their data is used, which would bring broad benefits to all concerned. Not least, we believe it is essential for the DM industry that the ICO is successful with its

objective of building public confidence in data protection by protecting people's identity and their data effectively.

Section 2: Scope of Personal Information Sharing

Q2: Key benefits (apply to individuals and society):

- Reduction in identity fraud from verifying data from multiple 'official' and up to date sources
- Improved marketing from greater targeting and higher data quality eg from using high quality sources of Government data such as register of births and deaths which will reduce volumes of 'junk' mail in UK and positive impact on the environment
- Improved public services from greater understanding of individual and local area needs from being able to analyse data from multiple sources and target individuals more precisely
- Improved law enforcement generally and especially important with the protection of children.

Q3: Key risks:

- Data loss and theft – numerous examples especially in the Government and Finance sectors - see our attached survey
- Broader misuse of personnel data leading to junk mail, spam and use of out of date listings in DM
- Less targeting by 'rogue' traders in DM
- Potential abuse of data in public sector.

Section 3: The Legal Framework

Q9 & Q12: The principles of the DPA are excellent. However, in our view the effectiveness of the Act could be greatly improved by:

1. Introducing data security breach legislation:

For example, public authorities and companies by law should have to make customers/prospects aware as soon as possible ('immediately') that their data has been compromised and to account to them and the ICO to show action has been taken to ensure it is highly unlikely to happen again and data subjects are appropriately compensated or assisted.

2. Enhanced powers for the ICO:

The Information Commissioner should be put on an equivalent footing to the Health & Safety Executive with powers to audit and fully investigate data loss and damage.

3. Significant Financial Penalties

Meaningful fines to be imposed on any company which falls foul of the Commissioner and ignores opt outs.

Section 4: Consent & Transparency

Q16: Consent in the Direct Marketing Industry

- We believe in consent and greater transparency. However, moving to a purely 'opt in' environment for direct marketing would have the reverse impact to the one intended. It would lead to limited coverage and make prospecting far less efficient driving advertisers to untargeted channels. This would increase the volume of wastage from media such as unaddressed mail, leaflets and inserts.
- The DM industry needs to take seriously consumer concerns about exercising their rights to opt-out by:
 - **Identification of Data Sources.** All prospect mailings should clearly indicate the name of the mailer and phone number which the recipient can call to amend or opt out of future mailings
 - **Centralised 'Do Not Contact' service.** Easy, fast and effective process for companies to handle calls from consumers to view, update or remove their details. Customers with data queries getting stuck at switchboard is too big a frustration to ignore
 - **Mandatory use of the Mail Preference Service (MPS).** The MPS should be on the same footing as TPS making it a statutory requirement to use this suppression file.

Section 5: Technology

Q20: Impact of Technology

- Lack of technology is no longer the issue – there are numerous effective encryption technologies being readily available on the market. Most problems occur due to human error and poor processes when handling data
- One technology that has proven **highly effective in the commercial data market** is **Data Tracking** where all list extracts are 'seeded' with unique names. Whilst this does not stop the data getting lost, it does highlight quickly if the lost or stolen data is used and by whom so that action can be taken quickly. We attach an example of how Yell Group plc has used data tracking to protect its valuable copyright in the High Court
- Hence, we believe it should be mandatory for all extracts of personnel data to include unique tracking addresses. It is quick, easy and inexpensive to implement.
- **Compliance auditing of (major) processors of personnel data in the public and private sector.** Recognising that most data loss and theft is down to human error we believe regular auditing, both overt and covert (mystery shopping), of business processes and systems should be carried out regularly on at least the major public bodies and private organisations that manage and process personnel data

- **Accreditation system for data processors in the Public & Private Sector.** In addition, an official accreditation programme should be set up for all public and commercial processors of personal data obliging them to undertake their trade with demanding standards for data protection and security. They should be effectively audited to maintain their accreditation status every year both covertly and overtly. Failure to reach required standards of care and security should prevent them from providing such services.

I hope this selective input is useful and do call if you would like to discuss any point.

Best regards.

Yours sincerely

Adrian Gregory
Managing Director