



Geodemographics in a digital age:

Ethical and data protection considerations

CGG Seminar

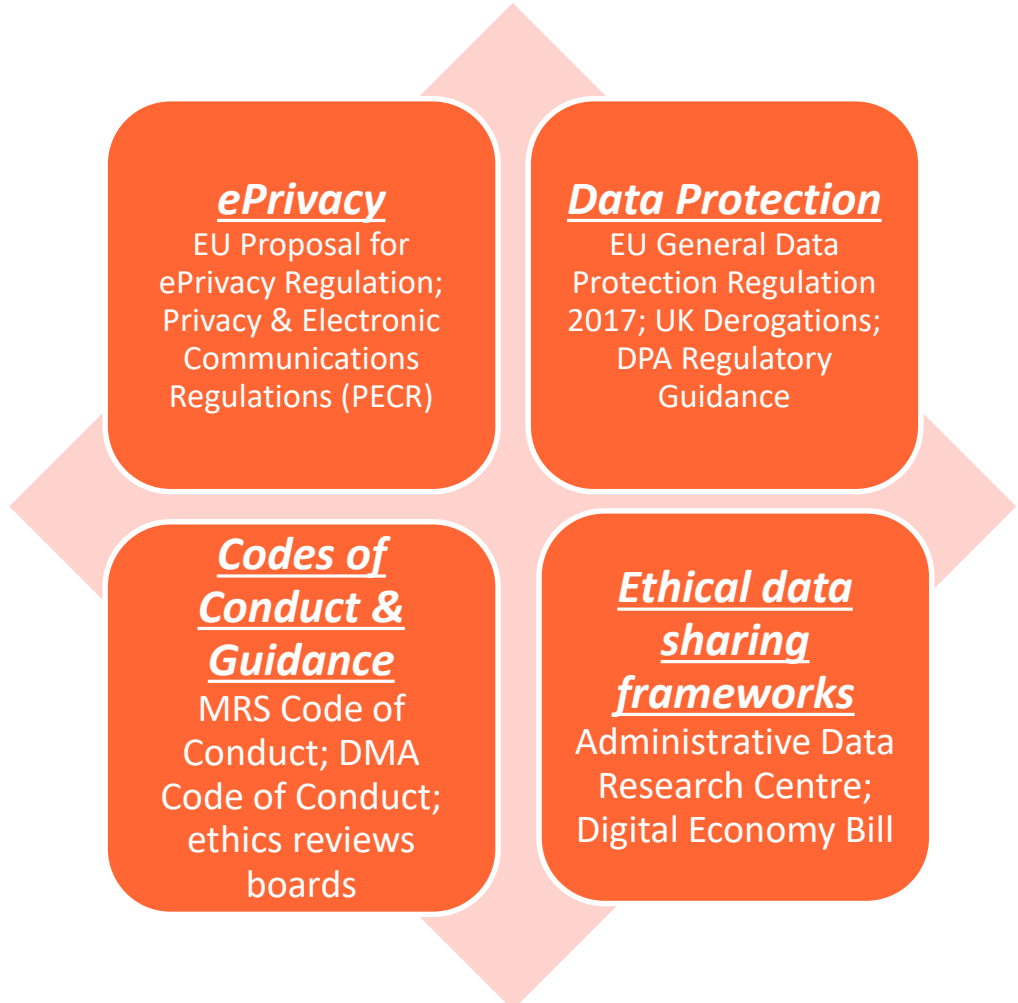
2nd May 2017

Dr. Michelle Goddard

Director of Policy & Standards



Complicated matrix of ethical and legal data protection requirements



Expanded definition of personal data in GDPR



Article 4

'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.

Geo-demographic data clear benefits but also legal risks



Data Project	Benefits (?)	Legal Considerations/Privacy Risks
<p>Online targeting for advertising merging geo-demographics categories, personal preferences, individual consumer behaviour</p>	<ul style="list-style-type: none"> • Broader insights and customer intelligence • More effective targeted advertising 	<ul style="list-style-type: none"> • ePrivacy - direct marketing regime consents • GDPR - right to object to DM & profiling • GDPR - appropriate grounds for primary and secondary processing • GDPR - risk assessment DPIA requirements • Privacy impact - Discrimination concerns • Privacy impact - Opacity of processing and limited individual controls
<p>Product development for a news service that captures IP addresses, GPS coordinates</p>	<ul style="list-style-type: none"> • Better customer experience • Targeted news relevant to location • Timely relevant news information alerts 	<ul style="list-style-type: none"> • GDPR – specific consent • GDPR - data minimisation
<p>Wi-fi location tracking in retail environment</p>	<ul style="list-style-type: none"> • Broader insights and customer intelligence 	<ul style="list-style-type: none"> • Uncertain impact of ePrivacy reforms • GDPR consents

Compliance tools & privacy solutions to achieve your data vision



Anonymisation

- Consider if personal data in dataset can be effectively anonymised or pseudonymised

Privacy Notices

- Use transparent privacy notices
- Be innovative in approach

Privacy impact assessment (PIA)

- Use PIA/DPIA to identify and mitigate privacy risks in a consultative process
- May be mandatory especially if using large dataset

Privacy by design approach

- Data protection by design and default is legal requirement
- Includes anonymisation; security measures; data minimisation; purpose limitation etc



**JUST
BECAUSE
YOU CAN
DOESN'T MEAN
YOU SHOULD!**