



IS GDPR GOOD OR BAD FOR BUSINESS?

Paul Winters, Managing Director, CACI Ltd.

16 January 2018



WE DO AMAZING
THINGS WITH DATA

1. GDPR: Overview
2. Consent
3. Legitimate Interest
4. Profiling
5. e-Privacy Regulation
6. Summary

GDPR: OVERVIEW

WHAT IS THE GENERAL DATA PROTECTION REGULATION?

- A new EU wide Regulation on data protection (173 Recitals and 99 articles)
- Harmonises individual rights on data protection across the EU
- Replaces the current Data Protection Act (DPA) of 1998
- A need to update existing legislation:
 - Much more data and the impact of digital channels and social media
 - Increased consumer awareness and concern about what happens to their data



HOW IS CACI PREPARING FOR GDPR?

1

SET UP GDPR
TASK FORCE

2

DATA AUDIT
OF ALL PII DATA

3

SUPPLIER DUE
DILIGENCE

4

DATA PROTECTION
IMPACT
ASSESSMENTS

5

NEW & REVISED
POLICIES

6

TRAINING &
AWARENESS FOR
STAFF

7

PLANNING FOR
CACI DATA
PRODUCTS

8

ECONOMIC IMPACT
ASSESSMENT
OF GDPR

9

INVOLVEMENT
IN THE DMA THIRD
PARTY DATA HUB

10

LOBBYING
POLITICIANS &
POLICY MAKERS

**GDPR IS
LONG OVERDUE**

**CACI ARE WELL
PREPARED**

WHAT'S NOT TO LIKE ABOUT GDPR?

SOME AREAS OF CONCERN FOR MARKETERS



CONSENT



**LEGITIMATE
INTEREST**



PROFILING



**E-PRIVACY
REGULATION**

THERE ARE SIX LAWFUL GROUNDS FOR PROCESSING PERSONAL DATA UNDER GDPR

1

CONSENT

2

CONTRACT
PERFORMANCE

3

LEGAL OBLIGATION

4

VITAL INTERESTS

5

PUBLIC INTEREST

6

LEGITIMATE INTEREST

GDPR explicitly recognises **direct marketing** as a **legitimate interest**

CONSENT

Under GDPR consent must be:

“Freely given...specific...informed...unambiguous...and given by a **statement or **clear affirmative action**”**

Pre-ticked boxes are banned as a way of obtaining consent

Third parties relying on consent must be **named at the point consent was given**

Unbundled (not hidden) and **granular** (separate consent for different processes)

Must be **easy for the data subject to withdraw consent**

New consents must be **sought** if current consent **does not meet** GDPR standards

- We believe that the ICO have taken an **overly restrictive view** of some of the GDPR clauses, e.g. that **opt-out boxes** will **no longer** be **valid** for **consent** purposes
- **CACI**, the **DMA** and many of **our competitors** have responded to the ICO consultation and **challenged** their **interpretation** of the **consent provisions** of GDPR
- Final guidance is expected in the next couple of months



POTENTIAL IMPACT ON BUSINESS OF STRICTER CONSENT REQUIREMENTS



“Over interpretation of consent provisions could reduce profits from data analytics and customer recruitment of **£150M** a year in the UK”

Consent will be almost impossible to achieve for customer acquisition

Entrench the power of big brands with consented databases & reduce competition & innovation

Less choice for consumers & more demand for consent

Big challenge for 3rd party data suppliers & their customers



“Opt in will cost us **tens of millions** of pounds”

LEGITIMATE INTEREST

LEGITIMATE INTEREST AS A LEGAL BASIS

“**Processing** will be **lawful** if it is **necessary** for the **purposes** of the **legitimate interests** pursued by the **controller** or a **third party**, **except** where such **interests** are **overridden** by the **interests** or **fundamental rights** and freedoms of the **data subject**....”

Article 6 (1) (f)

Must establish
that a **legitimate**
interest exists

Must establish
the **necessity**
of **processing**

Must perform a **balancing**
test to take account of
interests/ fundamental
rights of **data subjects**


“The **processing** of **Personal Data** for **direct marketing purposes** may be **regarded** as **carried out** for a **legitimate interest**”

PROBLEMS WITH LEGITIMATE INTEREST


Consent is objective but
Legitimate Interest is
more subjective

Lack of guidance from
regulatory authorities
about how they will
assess Legitimate Interest
in practice

Legitimate Interest not
recognised as a legal basis
for processing in the
ePrivacy draft



“You **won’t need consent** for **postal marketing** you can **rely** on **legitimate interests** for marketing activities if you can show how you use people’s data is **proportionate**, has a **minimal privacy impact**, and people would **not be surprised or likely to object.**”
(ICO web site, FAQs for charities)



The Third Party Data Hub is producing guidance on when **legitimate interest** can be used for **marketing involving 3rd party data.**

PROFILING

- Profiling is **explicitly mentioned** in GDPR as a form of **data processing** for the first time
- GDPR states that individuals have a **right not to be subject** to a **decision based on automated processing** that has a **legal** or **significant effect**
- **Profiling** is considered to be a form of “**automated processing**”
- The GDPR defines profiling as any form of automated processing intended to **evaluate** certain **personal aspects** of an **individual**, in particular to **analyse** or **predict** their:

PERFORMANCE
AT WORK

ECONOMIC
SITUATION

HEALTH

PERSONAL
PREFERENCES

RELIABILITY

BEHAVIOUR

LOCATION

MOVEMENTS

ISSUES AROUND PROFILING

Is the kind of **profiling** marketers carry out **likely** to have a “**legal or significant effect**” on the **data subject**?

How **much information** do we need to **give customers** about the **profiling we carry out** and will they **understand it**?

Is the kind of **profiling** marketers do “**automated processing**” or is there **some manual intervention**?

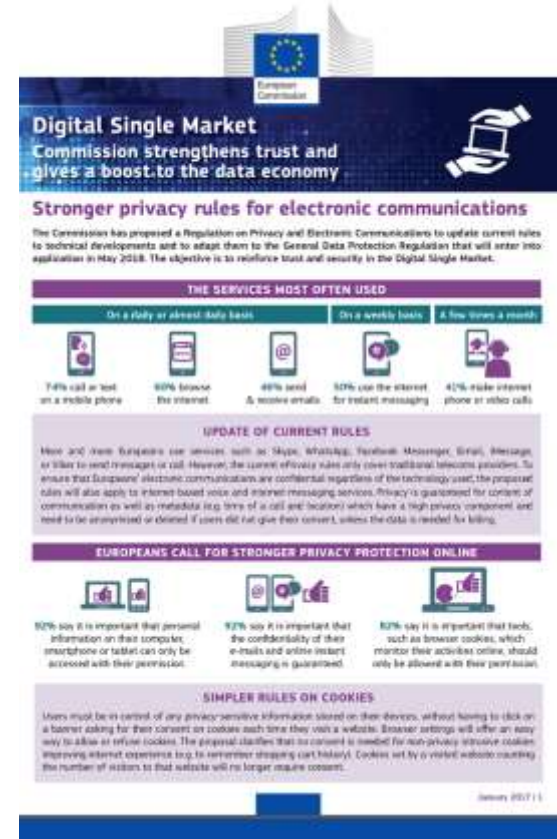
“In many typical cases **targeted advertising does not** have a **significant effect** on **individuals**...However, **it is possible** that it **may do**, depending upon the **particular characteristics of the case...**” (Guidelines on Automated individual decision-making and Profiling, Article 29 Working Party, October 2017)

The ICO is **still to issue** guidelines on profiling.

E-PRIVACY REGULATIONS

A NEW E-PRIVACY DIRECTIVE

- **PECR** (Privacy and Electronic Communications Regulation) was introduced in **2003** to **sit alongside** the **Data Protection Act**
- It gives additional **privacy rights to individuals** relating to **electronic communications** (emails, texts, telephone and fax and cookies)
- It is based on the EU ePrivacy Directive and was implemented across the EU
- It applies stricter rules on electronic marketing communications than other channels, e.g. consent must be opt-in
- A **new ePrivacy Directive** is being drafted in Brussels to sit alongside GDPR
- It will **update** the current ePrivacy Directive/PECR – **expected implementation in 2019**



A NEW E-PRIVACY DIRECTIVE

- The big issue is **consent** on **web sites** - how to **replace** the **cookie pop-up**
- Favoured route is via **web browser settings**
- Offer the consumer a choice from high to low levels of privacy such as :
 - Never accept cookies
 - Always accept cookies
 - Reject third party cookies
 - Only accept third party cookies from “favourite” brands
 - Only accept first party cookies
- New restrictions on **tracking locations** via **devices**, e.g. in shopping centres

- **Individual consent** for **cookies** could dramatically **affect online advertising revenues**
- This would **dramatically reduce free content** on the **web** and be **bad** for **consumers**

How workable is asking **browser manufacturers** to **solve the problem**?

Why can't **legitimate interest** be **used for online channels**?

A NEW E-PRIVACY DIRECTIVE: EXAMPLE COOKIES



65+
COOKIES DROPPED

SUMMARY

GDPR is a necessary & largely positive development

GDPR aimed for a balance between strengthening the data privacy rights of individuals and protecting the rights of business to process personal data as an engine of economic growth

GDPR largely gets the balance right but there are some areas of concern and uncertainty

The role of the ICO is critical: will they over-interpret and tip the balance away from business?