THE DATA PROTECTION ACT 2018
ORG: October 2018
chris.pounder@amberhawk.com
www.amberhawk.com

QUESTIONS?
• Do things like the GDPR genuinely help, or do they just make companies rewrite their privacy policies and continue doing what they always have?
• Compared to ten years ago, the average person on the street might now actually be aware that privacy is an issue. How significant is this? Ten years ago people weren’t asking for privacy, because they didn’t realize they didn’t have it. Now, people aren’t asking for privacy, because they don’t believe it’s possible to have. Is this progress?
• What are the privacy implications of various “rewards” schemes and loyalty programs? Barclays puts up billboards telling you to be careful who you share your data with, and then offers you a credit card with rewards from “selected partners.” Is this the pinnacle of hypocrisy?

QUESTIONS?
• What is the status of data that was collected before the GDPR came into effect, specifically data that should not be collected under the GDPR?
• Now that we have the GDPR, what can we and should we do practically with those rights? Hound companies to make them behave?
• What are companies and government institutions doing to undercut the GDPR and similar laws (e.g. the immigration exemption in the Data Protection Bill)?
WHY DO WE HAVE THE DPA 2018?


Articles where the Secretary of State has flexibility to amend the DPA 2018 (e.g. provisions in section 16 of the DPA)

STRUCTURE OF DP ACT

The Data Protection Act 1998 is repealed, but enforcement continues

The Data Protection Act 2018 is four Data Protection Acts

- UK’s implementation of GDPR for most Controllers
- UK’s implementation of Law Enforcement Directive for specified law enforcement bodies
- Data Protection for Spooks (Intelligence Services & GCHQ)
- Data Protection for none of the above (Applied GDPR; Brexit?)

Make sure you have the right regime

GDPR & BREXIT (UK as Third Country)

S.1(2) – “most” processing of personal data subject to the GDPR

“Guidance: Data protection if there’s no Brexit deal”, (13 Sept)
Under the heading “After March 2019 if there’s no deal”

- “There would be no immediate change in the UK’s own data protection standards. This is because the Data Protection Act 2018 would remain in place and the EU Withdrawal Act would incorporate the GDPR into UK law to sit alongside it”.

HOW THE GDPR/DP ACT 2018 WORKS?

1. Does the organisation process in a way that engages the Act?
   - Is the information processed “personal data”?
   - Is the organisation a “controller”?

2. If the Act is engaged then:
   - Is there a lawful basis to process personal data?
   - Is there a condition for processing of any special category of personal data or any criminal offence personal data?

3. If there is a lawful basis for the processing then:
   - How do we process? Apply the Data Protection Principles and other obligations (e.g. rights)

DEFINITIONAL POINTS

- **Personal Data** (information which relates to a living identifiable individual) (S.3(2))
- **Filing System** (has any structure)
- **Special category of personal data** (health, political, race, religion, trade unions etc); A.9(1) – SCPD is not a definition
- **Criminal offence personal data** includes alleged offences (S.11(2)) (Treated like SCPD).
- **Processing** (any operation on personal data such as use, retain, disclose, obtain) S.3(4))
- **Data Subject** (customers, employees, you) (S.3(5))
- **Controller** (purpose and means) (S.6(1); but note S.6(2))
- **Processor** (supplier processing on behalf of Controller); A.4(8)

LAWFUL PROCESSING (Article 6; LEGAL BASIS)

At least one **legal basis** has to apply to each processing operation:
- Data Subject consents
- **Necessary** for a contract in relation to the Data Subject or with a view to entering a contract
- **Necessary** for a legal obligation but not a contractual obligation
- **Necessary** in vital interests of Data Subject or another individual
- **Necessary** for performance of a task carried out in the public interest or in the exercise of the controller’s official authority
- **Necessary** in the legitimate interests of Controller, or in the legitimate interests of a Third Party to whom the personal data are disclosed, unless on a case-by-case basis, there is an overriding legitimate interests of the Data Subject.
MAJOR CHANGE RELATES TO LEGAL BASIS

- ICO rarely enforced “legal basis” under the First Principle of the DPA 1998 as it was in Schedule 2
- All A.6 bases are linked to the word “necessary”
- A.6 legal basis are part of the Transparency requirements
- Some rights are linked to the A.6 legal basis for processing
- Consent basis gives the data subject control of the processing

WHAT DOES “NECESSARY” MEAN?

- “It is well established in community law that, at least in the context of justification rather than derogation, “necessary” means “reasonably” rather than “absolutely or strictly necessary”
- the phrase “necessary in a democratic society” means that, to be compatible with the Convention (i.e. A.8, ECHR), the interference must... correspond to a "pressing social need" and be “proportionate to the legitimate aim pursued”.

DATA SUBJECT CONSENT

“consent” of data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to personal data relating to him or her being processed.

Direction of travel for ICO is “opt-in” for consent
- Tick the box if you want XYZ to happen [ ]
- NOT
- Tick the box if you do not want XYZ to happen [ ]
“GRITTED TEETH” CONSENT IS NOT CONSENT

• Consent in the employer-employee relationship? (e.g. “Will you show me your Facebook page?” at a job interview)
• Police ask you for an interview?
• Consent to go through the airport scanner after you have gone through airport security?
• Consent for disclosing criminal conviction data to get a job?

DATA SUBJECT CONSENT (A.7)

Burden of proof is on the controller to demonstrate that consent was given by the data subject.

The data subject shall have the right to withdraw his or her consent at any time (but does not have retrospective effect).

It shall be as easy to withdraw consent as to give it.

Right to withdraw consent is identified to data subjects (see A.13; A.14 next course).

CONSENT CHANGES (A.7; RECITALS 32, 42 & 43)

Consent clearly distinguishable from the other matters (e.g. other statutory notices).

Consent explained in an intelligible and easily accessible form, using clear & plain language (A.8; age appropriate if a child).

Any part of the consent declaration which constitutes an infringement of the DPA/Regulation can negate consent.

Recital 32: pre-ticked boxes do not constitute consent
Recital 42: Consent not valid if there is no effective choice
CONSENT (RECITALS 42)

Consent should not be regarded as freely given if:

• it does not allow separate consent to be given to different personal data processing operations
• the data subject is unable to refuse or withdraw consent without detriment or has no genuine or free choice
• performance of a contract dependent on consent despite such consent not being necessary for such performance. (e.g. “By signing this contract you consent to...” is suspect)

Controller to demonstrate that the data subject has given consent to the processing operation

“NECESSARY” & DATA SUBJECT CONSENT

Data Minimisation (third) Principle (A.5(1)(c)):

• adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

Storage Limitation (fifth) Principle (A.5(1)(e)):

• kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed

• A.6 legal bases are “necessary” for something except for consent; the Principles above link “necessary” to consent

SOME ARTICLE 9 CONDITIONS FOR SPECIAL CATEGORIES OF PERSONAL DATA

• Data subject has given explicit consent
• Necessary obligations/rights of the controller or of the data subject in the field of employment and social security law
• Necessary for vital interests of data subject or other individual
• Manifestly made public by the data subject
• Necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity
• Necessary for scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based
MORE SPECIAL CATEGORY CONDITIONS (Schedule 1, Part 1 & Part 2)
Conditions link to “substantial public interest” unless italicised
• Employment, social security and social protection
• Health or social care purposes
• Public health in the public interest
• Research and archiving in the public interest
• Necessary for statutory and public sector functions
• Administration of justice and parliamentary purposes
• Equality of opportunity or treatment
• Racial and ethnic diversity at senior levels of organisations
• Counselling
• Safeguarding of children and of individuals at risk
  (and policy document)

MORE SPECIAL CATEGORY CONDITIONS (Schedule 1, Part 2)
Conditions link to “substantial public interest” unless italicised
• Preventing or detecting unlawful acts (but if the processing is only for disclosure to a competent authority then no policy document)
• Protecting the public against dishonesty etc
• Regulatory requirements relating to unlawful acts & dishonesty
• Special Purpose in connection with unlawful acts & dishonesty
• Preventing fraud (by an anti-fraud organisation such as CIFAS)
• Suspicion of terrorist financing or money laundering
• Support for individuals with a particular disability or medical condition by a not-for profit
• Safeguarding economic well-being of certain individuals (e.g. vulnerable adults with Alzheimers)
  (and policy document)

MORE SPECIAL CATEGORY CONDITIONS (Schedule 1, Part 2)
Conditions link to “substantial public interest” unless italicised
• Insurance condition
• Occupational pensions
• Political parties
• Elected representatives responding to requests
• Disclosure to elected representatives
• Informing elected representatives about (release of) prisoners
• Publication of legal judgments
• Anti-doping in sport
• Standards of behaviour in sport
  (and policy document)
A.20-A.22 RIGHTS AND A.6 LEGAL BASIS

Right to data portability (A.20)
- Consent (A.6(1)(a))
- Contract (A.6(1)(b))

Right to object (A.21)
- public task (A.6(1)(e))
- legitimate interests (A.6(1)(f))

Right to object to marketing (A.21)
- consent; (A.6(1)(a))
- legitimate interests (A.6(1)(f))

Prohibition on automated decisions & profiling lifted... (A.22)
- consent (A.6(1)(a))
- contract (A.6(1)(b))
- required by law (A.6(1)(c) & S.14(3)(c))

RIGHT TO ERASURE AND A.6

Right to erasure applies (A.17)
- Consent withdrawn (A.6(1)(a))
- Legal obligation to delete (A.6(1)(c))
- Balance of interests in favour of the data subject (A.6(1)(f))
- No A.6 grounds for processing

Right to erasure does not apply
- If necessary to protect freedom of speech
- Legal obligation to retain (A.6(1)(c))
- Necessary for a public task (A.6(1)(e))
- Balance of interest in favour of the controller (A.6(1)(f))

Right to be informed (A.13/A.14) identifies legal basis to data subjects

TRANSPARENCY NOTICE (A.13/A.14) SPECIFIES LEGAL BASIS FOR PROCESSING

"THE RIGHT TO BE INFORMED" includes the following detail which has to be given to the data subject (unless there is an exemption):
- the purposes of the processing for which the personal data are intended as well as the A.6 legal basis of the processing
- Awareness of all rights (some are linked to the A.6 basis)
- where the processing is based on the A.6 basis of consent, the existence of the right to withdraw consent at any time
- Whether provision of personal data is a statutory or contractual requirement, whether provision is an obligation, and consequences if failure to provide - (i.e. what is "necessary")
ACCOUNTABILITY (A.5(2); A.24)
The controller shall be responsible for, and be able to demonstrate compliance with the Principles (accountability; A.5(2))

...the controller shall (...) implement appropriate measures and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation” (A.24(1))

Need evidence of compliance with Principles.
Information subject to FOIA/FOISA in public sector

(FIRST) PRINCIPLE (‘lawfulness, fairness and transparency ’; A.5(1)(a))

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject;

Three limbs to the First Principle:

- **Lawful** processing of personal data (e.g. accords with a statutory obligation, vires, not breaching confidentiality, copyright);
- **Fair** processing of personal data (e.g. outcome of processing non-discriminatory in general)
- **Transparent** processing of personal data (providing the data subject with information about the processing)

RIGHT TO BE INFORMED (A.13, A.14)
THE SET {X} MUST BE PROVIDED

Must provide in all circumstances (unless an exemption applies):

- the identity and contact details of the controller
- Contact details for any data protection officer
- the purposes of the processing for which the personal data are intended as well as the A.6 legal basis of the processing
- Recipients or categories of recipients
- Intention to transfer of personal data to a recipient in a third country
RIGHT TO BE INFORMED (A.13, A.14)
THE SET \{Y\} MIGHT BE PROVIDED

Given where necessary (unless an exemption applies):

- the period for which the personal data will be stored, or if this is not possible, the criteria used to determine retention;
- where the processing is based on consent, the existence of the right to withdraw consent at any time;
- awareness of all relevant rights (e.g. access, portability, object);
- whether provision of personal data is a statutory or contractual requirement, whether provision is an obligation, and consequences if failure to provide the personal data;
- the right to lodge a complaint to a supervisory authority;
- the existence of automated decision making including profiling logic involved, and impact on the data subject.

RIGHT TO BE INFORMED (A.14)
THE SET \{Z\} – ADDITIONAL DETAILS

Only when personal data are collected from other sources (Does not apply if personal data obtained from the data subject)

MUST be provided (unless an exemption applies):

- The categories of personal data concerned.

MIGHT be provided (unless an exemption applies):

- Where processing is based on legitimate interest(s) pursued by the controller or by the third party details of those interest(s);
- Details concerning the source of the information, including publicly accessible sources.

(SECOND) PRINCIPLE (‘Purpose Limitation’; A.5(1)(b))

Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

- Purpose of collection usually specified to the data subject as part of the right to be informed; legitimate is the A.6 basis.
- What happens if the further processing is “incompatible”?
- If a further purpose is intended it has to be compared with the purpose of obtaining to assess whether it is incompatible.
- So keeping copies of what has been provided to data subjects and when becomes important (e.g. on web-sites).
A FURTHER COMPATIBLE PURPOSE? (A.6(4))

Controller wants to use personal data for some further purpose
- Consent or Member State law in A.23(1) equals compatible
Assessment of "compatibility" involves consideration of:
- Links between the purpose of obtaining and further purpose
- Context of personal data collected
- Relationship between data subject and controller
- Nature of personal data (e.g. care with A.9 data implied)
- Consequences of further processing
- Safeguarding measures for data subjects (e.g. the use of encryption or pseudonymisation)

A “further” purpose engages A.13 & A.14; contact with data subject might be needed (see Transparency Principle A.5(1)(a))

THE END

More on the GDPR in all DP courses .... and on HAWKTALK (wholly balanced blog)

©Chris Slane