THE CHURCH OF ENGLAND
NATIONAL CHURCH INSTITUTIONS

GDPR and Consent

(includes slides 21- 22 that are specific to CMS)

Madi McAllister
Information Governance Officer

Note: This presentation is guidance only, and should not be read as legal advice

THE CHURCH OF ENGLAND
NATIONAL CHURCH INSTITUTIONS

Concepts

- Definition of consent:
  - "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 the processing of personal relating to him or her."
- Fundamental right
  - One of 6 lawful bases for processing person data
- Informed consent
  - Gives data subject control over whether or not their personal data will be processed
  - If not freely given, control is not present and consent will be on an invalid basis, rending the processing activity unlawful.
  - Consent doesn't legitimise data collection if it isn't fair, proportionate and necessary
- Only appropriate when:
  - Data subject is in control
  - Has been offered a genuine choice to accept or decline the terms offered
  - Can decline without detriment
- Explicit consent
  - One of the exemptions to the prohibition of processing special categories of personal data.

THE CHURCH OF ENGLAND
NATIONAL CHURCH INSTITUTIONS

Components

- Validity
- Imbalance of power
- Bundling
- Choice without detriment
- Informed
- Specific
- Affirmative
- Explicit
- Withdrawal
- Renewal
- Effect on individual rights

THE CHURCH OF ENGLAND
NATIONAL CHURCH INSTITUTIONS

Valid consent

- Free/freely given
  - Implies real choice and control
- Will not meet this standard if:
  - The data subject feels compelled or will endure negative consequences if they do not consent
  - Consent is bundled up in a non-negotiable part of Terms and Conditions
  - Unable to refuse or withdraw consent without detriment
  - There is a risk of deception, intimidation, coercion or significant negative consequences (e.g. extra costs to individual) if he/she doesn't consent.
  - Where there is any element of compulsion, pressure or inability to exercise free will.
  - Where an imbalance exists between controller and data subject (health records, employment)
- Valid consent always preceded by determination of:
  - Specific – what purpose is being consented to; clear separation of information needing consent from information that doesn't
  - Explicit – active choice by data subject
  - Legitimate – be the correct lawful basis.

THE CHURCH OF ENGLAND
NATIONAL CHURCH INSTITUTIONS

Imbalance of power

- Imbalance of power between employer and data subject/employee
  - e.g. Can't respond freely to a request for consent to activate monitoring systems such as CCTV in the work place, or to complete assessment forms – without feeling pressure to consent
- For the majority of processing at work, the lawful basis cannot and should not be consent of employees
- Exceptional circumstances:
  - e.g. a film crew wants to film in a certain part of the building, employees not wishing to be filmed can be moved to a different part of the building
- Most data processing for employment purposes is necessary for the performance of a contract – e.g. processing of salary and bank account details so employee can be paid – therefore consent is not the lawful basis.

THE CHURCH OF ENGLAND
NATIONAL CHURCH INSTITUTIONS

Bundling consent

- Should not bundle consent into acceptance of terms or conditions
  - Tying the provision of a contract or a service to a request for consent for data that are not necessary for the provision of that contract or service
- Cannot be mandatory in exchange for performance of a contract or service
  - It equates to compulsion to agree to what is not strictly necessary
  - If the data subject does not consent, runs the risk of being denied the services they have requested
  - If consent is given – presumed to be not freely given
- If using "performance of a contract" as lawful basis:
  - Determine the scope of the contract or service – processing must be necessary to fulfil the contract for each individual data subject
  - No need for additional basis of consent except if your data requirement includes special categories, and contract is not a legal basis for this
- e.g. if a bank asks customers for consent to use details for marketing (which they do) – if refusal to that means closure of the bank account, consent is not a lawful basis (legal aid).

THE CHURCH OF ENGLAND
NATIONAL CHURCH INSTITUTIONS

Choice in contract / service

- Could provide real choice, if:
  - The data subject can choose between a service that includes consenting for additional purposes; AND
  - You are providing an equivalent service that doesn't include consent for additional purposes
- Must be possible for the data subject to have the contract or service performed without consenting to the other or additional use of data
- But both services must be genuinely equivalent.

THE CHURCH OF ENGLAND
NATIONAL CHURCH INSTITUTIONS

Informed consent (1)

Elements that are crucial to make a choice:

- The information must be clear and accessible, understandable by an average person, not written in legalese or statements full of legal jargon

1. Controllers identity
   - Where consent will be relied on by multiple (joint) data controllers – all organisations should be named (If data will be transferred to other data controllers who wish to rely on the original consent)
2. Purpose of each processing operation for which consent is being sought
3. What type of data will be collected and used
4. The existence of the right to withdraw consent
5. List or recipients or data processors or other data controllers
6. Information about the use of data for automatic processing or profiling/ or not
7. If the consent relates to transfer, information about the possible risks of transfers to 3rd countries in the absence of adequate safeguards.

THE CHURCH OF ENGLAND
NATIONAL CHURCH INSTITUTIONS

Informed consent (2)

- Consent must be clearly and distinguishable from other matters
- Not hidden in general terms and conditions
- Easy to identify the data controller, purpose for processing
- Can be layered (electronic)
  - Main statement on header page, with details available via a hyperlink
  - BUT – actual consent statement must be clear and definable
  - BUT identity of controller and purpose of processing must be on header page, as data subject may not read any further
- Decide what information is necessary for the specific audience (e.g. children) and present it appropriately
- Declaration of consent must be named as such
  - e.g. "By giving us this information you understand that…" is not clear language
- Can achieve valid, informed, consent without necessarily meeting PN requirements
  - e.g. not provide name of DPO, not provide retention period

THE CHURCH OF ENGLAND
NATIONAL CHURCH INSTITUTIONS

Consent vs Privacy Notices

- Identity and contact details of the controller
- Purpose of the processing and the lawful basis for the processing
- The right to withdraw consent at any time, where relevant

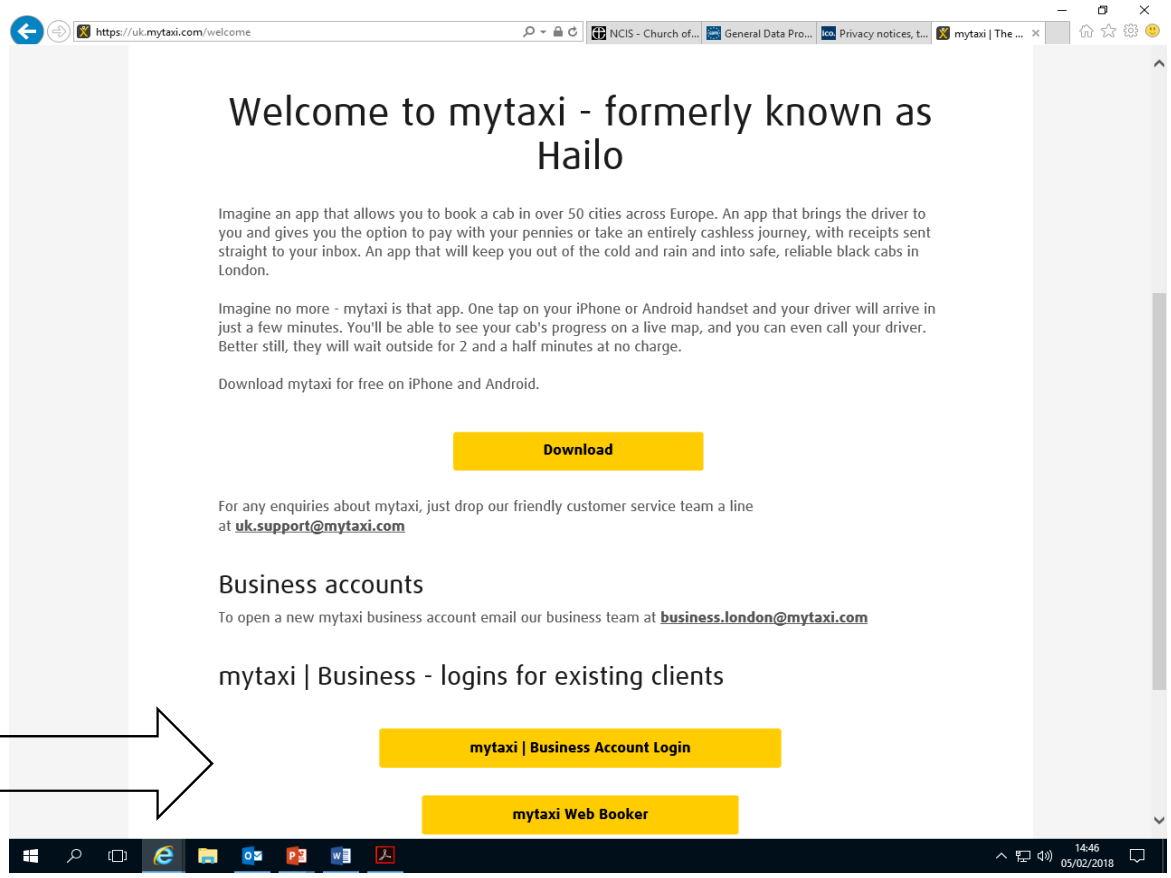
- The data protection officer
- Categories of personal data
- Any recipient or categories of recipients of the personal data
- Details of transfers to third country and safeguards
- Retention period or criteria used to determine the retention period
- The existence of each of data subject's rights
- The right to lodge a complaint with a supervisory authority
- The source the personal data originates from and whether it came from publicly accessible sources
- Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data
- The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences

THE CHURCH OF ENGLAND
NATIONAL CHURCH INSTITUTIONS

Layered Consent Notice?

- "1.2 Prior to using the mytaxi Services, the passenger must register. Registration requires the passenger's correct and full first and last name, email address ("user name"), mailing address, phone number and login password. All personal data provided by the passenger to mytaxi will be processed in accordance with the Privacy Policy accessible at www.mytaxi.com."

If you follow the link – you get to this page – where there is no Privacy Policy to be found!



THE CHURCH OF ENGLAND
NATIONAL CHURCH INSTITUTIONS

Specific

- Service could involve multiple processing operations with more than one purpose
- Data subject must be free to choose:
  - Which purpose they accept
  - Which data they want to consent to processing and which they do not
- Must not ask data subject to consent to the whole bundle
- Several consents may be warranted to start offering the service
  - e.g. Consent to receive a newsletter from you and another 3rd party is two separate purposes
- If you can't offer this choice, then consent is not freely given
- So consent must be specific
  - A separation of different purposes and obtaining consent for each purpose
- Can have a single consent that covers multiple processing – as long as they all have the same purpose.
  - e.g. Data subject completes a paper form (2), received by administrator and data input into electronic database (1) and paper form filed in filing cabinet, electronic data downloaded into spreadsheet (3).

THE CHURCH OF ENGLAND
NATIONAL CHURCH INSTITUTIONS

Affirmative consent

- Must take a deliberate action (written, recorded oral statement)
- Must not be obtained in the same motion (e.g. swiping a phone screen) as agreeing a contract or terms and conditions of a service
  - This is not a clear affirmative action of consent to use of data.
- No pre-ticked boxes or opt out boxes that require the data subject to intervene to prevent agreement.

THE CHURCH OF ENGLAND
NATIONAL CHURCH INSTITUTIONS

Explicit consent

- Explicit consent exists to manage occasions where serious data protection risk emerges and a high level of individual control over personal data is appropriate
- Explicit consent:
  - The way consent is expressed
  - Data subject must give an express statement
  - The controller can ask for expressly confirmed consent in writing, signed by the data subject
- Is a second level of lawful reason required when:
  - Processing special categories of personal data
  - Transferring to third countries or international organisations in the absence of adequate safeguards (as long as not on an on-going basis)
  - Using automated decision making and profiling.

THE CHURCH OF ENGLAND
NATIONAL CHURCH INSTITUTIONS

Valid consent?

1. "Privacy Notice

We need to hold your information about you and your dependents, to enable us to operate the pension scheme. This information will only be shared with third parties who help us to administer the scheme, such as the Scheme Auditor, the Scheme Actuary and our other professional advisers."

Q: Is this sufficient information for valid consent?

2. "The Scheme Manager will use this information when you visit the scheme for your assessment. The assessment at the scheme is also an opportunity for you to raise any concerns or queries you may have. In a few cases, we may need to contact your Doctor for further information. We need your permission to do this and ask that you sign the consent below.

I authorise the xxx (name of organisation) to contact my doctor and/or hospital consultant in order to make a medical assessment concerning my housing application."

Q: This concerns health data which requires explicit consent.

THE CHURCH OF ENGLAND
NATIONAL CHURCH INSTITUTIONS

Withdrawal

- Must be as easy as giving consent
  - But not necessarily in the same way or through the same action
  - If doing it electronically - can't switch methods so as to require more effort
- Must be free of charge and no change in service levels
- Must tell data subject there is a right to withdraw prior to processing
- If none of these are applied then consent is not valid
- If consent is withdrawn
  - Does not make processing operation unlawful, but
  - Must stop the processing actions concerned if no other legal basis is in place
  - Data must be deleted or anonymised
  - Can continue with processing of data that is already under another lawful basis e.g. contract
- If want to continue with another lawful basis, cannot silently migrate data to this other basis
  - Any change to the lawful basis must be notified to data subject.
- Recording withdrawal - must keep record of withdrawal and of processing stopped
  - If you just delete all reference to that person, may approach them again inadvertently
  - You need to know what has been deleted in the case of an SAR.

THE CHURCH OF ENGLAND
NATIONAL CHURCH INSTITUTIONS

Renewal of consent

- How long does consent last?
  - If processing operation changes or evolve significantly – original consent no longer valid and new needed
  - Retention once processing operation ends, consent should be kept no longer that strictly necessary for compliance with legal obligation or exercise/defence of legal claims.
- Best practice is to refresh at appropriate intervals
  - Provide all info again so data subject kept well informed
- Where using consent under DPA 1998, not automatically required to completely refresh all existing consent relations
  - Existing consent continues to be valid if in line with GDPR conditions
- Should review existing consent standards/forms and mechanisms, including withdrawal:
  - No longer allowed to have presumed consent where no record kept = must be renewed
  - Implied actions (ignoring a pre-ticked box) = must be renewed
- BUT – if the existing consent is not applicable, consider another lawful basis
  - Only allowed in transition to GDPR. Once GDPR applies, can't swap between lawful bases
- If no other lawful basis exists – must cease processing until consent renewed

THE CHURCH OF ENGLAND
NATIONAL CHURCH INSTITUTIONS

Effect on individual rights

- Data that is processed solely on consent, gives the data subject the following rights:
  - Portability
  - Erasure
  - Be forgotten where consent withdrawn
  - Restriction
  - Rectification
  - Access
- No right to object – withdrawal will have same result

THE CHURCH OF ENGLAND
NATIONAL CHURCH INSTITUTIONS

In summary

- Data controller must:
  - Assess validity
  - Determine if processing can be lawfully carried out under any other lawful basis
  - Obtain consent prior to processing being carried out
  - Obtain written explicit consent for special categories
  - Record and retain for the length of time the processing exists
  - Provide mechanisms for withdrawal
- Must be able to demonstrate:
  - Consent was received
  - How (mechanism)
  - When
  - Information provided at the time (onus on controller to keep policies, snapshots of websites etc over time – to demonstrate what was in place when consent was received).
  - That the data subject was informed
  - That consent was valid

Data processor:

- Will rely on data controller to have collected the data appropriately.
- Has no obligation to check that consent is valid or present.

THE CHURCH OF ENGLAND
NATIONAL CHURCH INSTITUTIONS

Marketing

- Definition
  - all advertising or promotional material, including that promoting the aims or ideals of not-for-profit organisations
- Marketing is allowed! (Recital 47 – legitimate interest use of personal data)
- The marketing must be directed to particular individuals. In practice, email messages are directed to someone, so they fall within this definition
- If using email - falls under the Privacy and Electronic Communications Regulations 2003 (PECR)
- You can only carry out unsolicited electronic marketing if the person you're targeting has given you their permission (consent)
- An unsolicited message is any message that has not been specifically requested. So even if the customer has 'opted in' to receiving marketing from you, it still counts as unsolicited marketing.
- An opt-in means the customer agrees to future messages (and is likely to mean that the marketing complies with PECR). But this is not the same as someone specifically contacting you to ask for particular information (solicited marking – unrestricted).

THE CHURCH OF ENGLAND
NATIONAL CHURCH INSTITUTIONS

CMS privacy settings

- Consent to sharing/disclosure
- What are the purposes of processing? CMS has multiple purposes.
- Is consent the most appropriate lawful purpose?
    - Private
    - Diocese
    - Public

THE CHURCH OF ENGLAND
NATIONAL CHURCH INSTITUTIONS

Suspense Procedure

- Is this necessary for all new entries/contacts?

- Yes
  - Provides fair and transparent processing
  - Informs data subject, checks data accuracy
  - Requests consent for sharing (where relevant)

- No
  - If data is already held in another format and being transferred to CMS
  - If consent is necessary and already held and valid