

● ● ●  
● ● ● cornerstone  
● ● ● barristers

GDPR 2 years on - Lessons learned and  
practical tips for compliance

Estelle Dehon, Matt Lewin, Ruchi Parekh, John Fitzsimons,  
Dr Christina Lienen, Olivia Davies

22 June 2020

# Overview




**Transparency and accountability**

**Challenges with DPIAs and DP policies**

**Engaging with the ICO**

**The next two years: Covid-19 & Brexit**



# Transparency and accountability

# Transparency under the GDPR



**ICO Guidance**

**Article 5(1) GDPR**

**Recital 39**

# Website privacy notice



- A privacy notice is a document made publicly available by an organisation that explains how that organisation processes personal data in a GDPR compliant way
- If you are collecting personal data directly from someone, e.g. through an online contact form or account, you have to provide them with your privacy notice at the moment you do so

The screenshot shows the footer of the Information Commissioner's Office (ICO) website. The footer is dark blue with white text. It includes the ICO logo on the left, followed by a navigation menu with links: 'Your data matters', 'For organisations', 'Action we've taken', and 'About the ICO'. Below these are sub-links: 'Official information', 'Nuisance calls', 'Guide to Data Protection', 'Guide to FOI', 'Guide to PECR', 'Enforcement action', 'Decision notices', 'Audits', 'Who we are', 'What we do', 'News and events', and 'Jobs'. At the bottom, there is a dark blue bar with white text: '© Copyright', 'Privacy notice', 'Cookies', 'Disclaimer', 'Publications', 'Accessibility', and 'Contact us'. The 'Privacy notice' link is circled in pink. Below this bar is a white bar with a search icon and the text 'Type here to search'. At the bottom of the screen is the Windows taskbar with various application icons and the system tray showing the time '11:50' and date '19/06/2020'.

# How the GDPR's transparency requirement affects website privacy notices





## A selection of important things you need to do to achieve and demonstrate compliance

1. You need to tell data subjects the legal basis for data processing (Arts. 5(1)(a) and 6(1) GDPR)
2. If you rely on 'legitimate interests' as a legal basis, you must provide details of those legitimate interests (Art. 13(1)(d) GDPR)
3. You need to inform data subjects about their rights, e.g. right of erasure (Art. 13(2)(b) GDPR)
4. You need to identify - ideally by name, otherwise by reference to category - any recipients of the personal data you collect (Art. 13(1)(e) GDPR)
5. You need to tell data subjects if any of the data processing will take place outside the EEA, e.g. on US servers, and what safeguards have been put in place (Art. 13(1)(f) GDPR)

# Top tips for drafting a GDPR compliant privacy notice



1. The more you prep, the easier it gets
2. Be transparent and precise
  -  “We may use some of your personal data to offer you personalised services”
  -  “We will retain your order and browsing history to make suggestions to you for other products which we believe you will also be interested in”
3. **When** (do you process), **What** (do you process), **Why** (do you process), **What** (legal basis are you relying on)?
4. Consider adopting a layered approach

# What about cookies? 🍪



If you use cookies or similar tracking technologies, e.g. HTML 5 local storage, web bugs, tracking pixels or device fingerprinting on your website, you need to cover this in your privacy notice either:

- (a) Under a dedicated section in the privacy notice, or
- (b) In a separate cookies policy notice, or
- (c) A combination of both

Explaining your usage of cookies in this way does not amount to obtaining consent for the placing of cookies as required by PECR 2003 or the GDPR – a separate mechanism is required for valid consent



# What are cookies? 🍪



- Cookies are small data files stored on a user's computer, phone or tablet. They allow an online service, such as a website, to recognise an individual user and store certain information about them such as login details, the contents of shopping baskets and site preferences
- Regulated by:
  - The Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR 2003), which transposed Directive 2002/58/EC (the ePrivacy Directive) into UK law
  - The GDPR

# e-Privacy Directive 2002/58/EC – the requirement for consent to cookies



- Article 5(3):

*“Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive [95/46], inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service”*

# *Verbraucherzentrale Bundesverband v Planet 49: ECJ case C-673/17*



- Planet 49 ran a promotional lottery on its website
- Users were presented with two tick-boxes:
  - 1) An unchecked tick-box to receive third party advertising
  - 2) A pre-ticked check box to set cookies
- 4 significant points arose from the judgment

# 1) Pre-ticked check boxes authorising the use of cookies are not valid consent



- The court interpreted the phrase “given his or her consent” in article 5(3) literally – the phrase requires action on the part of the user
- Consent may be given by any appropriate method enabling a freely given specific and informed indication of the user’s wishes, including ‘by ticking a box when visiting an internet website’
- Only active behaviour on the part of the user is sufficient
- A pre-selected tick box does not imply active behavior

## 2) The standard of consent under the e-privacy directive is the GDPR standard



- GDPR now expressly requires active consent and precludes 'silence, pre-ticked boxes or inactivity' from constituting consent (recital 32)
- Article 5(3) of the e-privacy directive must be read in conjunction with Article 4(11) of the GDPR
- Consent must be:
  - 1) Freely given
  - 2) Specific
  - 3) Informed
  - 4) An unambiguous indication of the data subject's wishes by which they, by a statement/clear affirmative action, signify agreement to the processing of their personal data

### 3) Article 5(3) applies regardless of whether cookies are personal data



- Article 5(3) does not refer to personal data
- Article 5(3) aims to protect from interference with the “private sphere” regardless of whether personal data is involved
- The definition of “private sphere” in Recital 24 of the e-privacy directive supports this interpretation

## 4) Users must be informed of the duration of cookies, and whether third parties will have access to them



- The “clear and comprehensive information” required by article 5(3) implies that a user can easily determine the consequences of any consent they might give and ensure that the consent given is well informed
- The duration of the operation of the cookies and whether or not third parties may have access to those cookies form part of the clear and comprehensive information required under Article 5(3)



# Updated EDPB Guidelines on consent – May 2020



- Conditionality –

*"for consent to be freely given, access to services and functionalities must not be made conditional on the consent of a user to the storing of information, or gaining of access to information already stored, in the terminal equipment of a user (so-called cookie walls)" (paragraph 39)*

- Unambiguous indication of wishes –

*"Scrolling or swiping through a webpage or similar user activity will not under any circumstances satisfy the requirement of a clear and affirmative action" (paragraph 86)*



# Top tips for compliance with the consent requirement



- Require clear, affirmative action by the user
- Consider your website's complexity
- Timing – consent must be gained before cookies are used
- No consent by 'default':
  - ✗ Pre-ticked boxes
  - ✗ Sliders set to 'on'
  - ✗ "Accept" button with no option to reject
- No "conditional" provision of services/functionality:
  - ✗ Cookie walls



# Challenges with DPIAs and data protection policies

# Data Protection Impact Assessment



## Areas of challenge

**When to carry  
out a DPIA**

**Publishing  
DPIAs**

# When to carry out a DPIA



**Risk profile**

**Processing ...  
likely to result  
in a high risk to  
rights and  
freedoms**

**'High risk'**

# Data Protection Impact Assessment



## Risk profile

**What risks?**

**Severity?**

**Likelihood?**

**Controls?**

# When to carry out a DPIA



**Risk profile**

**Processing ...  
likely to result in  
a high risk to  
rights and  
freedoms**

**'High risk'**

# Data Protection Impact Assessment



**High risk**

**Articles 35(1)  
and (3)**

**A29WP:  
9 guidelines**

**ICO:  
List of 10  
activities**

# Data Protection Impact Assessment



## Areas of challenge

**When to  
carry out a  
DPIA**

**Publishing  
DPIAs**



# Data Protection Impact Assessment



Duty to publish?

**Consultation**

**Accountability**

# Data protection policies



**Devices**

**Video  
conferencing**

**Working  
from home**

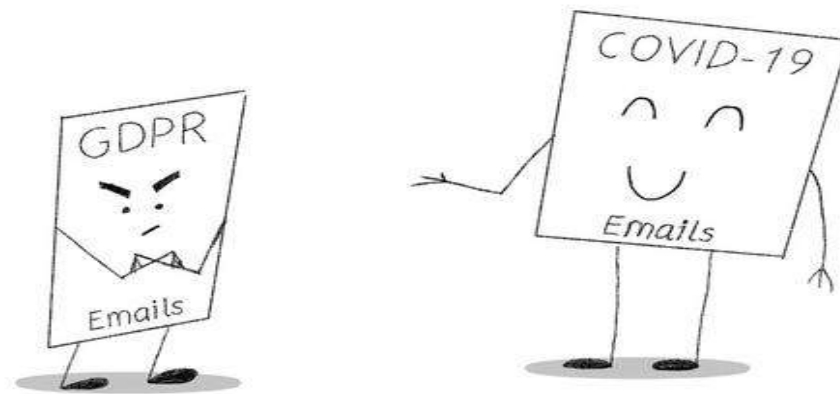
**Data storage**

**Communication**



# Engaging with the ICO

# Regulation during a pandemic



*You're still more annoying ...*

*@itslikethisonly*

# Regulation during a pandemic



ICO's Regulatory Approach: *“The coronavirus public health emergency means that we must reassess our priorities and our own resourcing, so that we retain the right balance in these challenging times, focusing on those areas that are likely to cause the greatest public harm”*

**Staff and  
Operating  
capacity  
shortages**

**Public sector  
face front-line  
pressures and  
redeploying  
accordingly**

**Acute financial  
pressures**

# Regulation during a pandemic



*ICO's Regulatory Approach: "As a public authority, we must act in a manner which takes into account these circumstances...we are committed to an empathetic and pragmatic approach, and will demonstrate this through our actions."*

**Focus on  
most serious  
challenges  
and greatest  
public threats**

**Flexible  
approach,  
taking account  
of economic or  
resource  
burdens**

**Firm action  
against those  
exploiting the  
emergency**

# Regulation during a pandemic



## GDPR?

- Still a duty to report within 72 hours but “we acknowledge that the current crisis may impact this”
- “Empathetic and proportionate approach” to reports
- Breach investigations:
  - How has the crisis impacted an organisation (i.e. do GDPR difficulties arise as a result of the crisis)
  - Any fines will take account of economic impact of crisis
  - Recognise that SAR response times may be impacted

## FOI/EIR?

- Still accepting new information complaints but recognise that reduction in resources = impact on response times
- Should still seek “as far as possible...to comply with obligations for particularly high-risk or high profile matters.
- Importance of proper record keeping during a period of time that will be subject to future public scrutiny.

# Regulation during a pandemic



What  
next?

- “Coronavirus recovery – six data protection steps for organisations”:
  - Only collecting and using what is necessary
  - Keeping collection to a minimum
  - Clarity, honesty and openness with staff about use of their data
  - Treating people fairly
  - Securing information
  - Ensuring staff can exercise their information rights



# Regulation during a pandemic



**Protecting our  
vulnerable  
citizens**

**Supporting  
economic  
growth and  
digitalisation,  
including small  
businesses**

**Shaping  
proportionate  
surveillance**

**Enabling good  
practice in AI**

**Enabling  
transparency**

**Maintainig  
business  
continuity**

# Personal data breaches



# Personal data breaches



***Personal data breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*

**Internal  
recording**

**Notifying  
the ICO**

**Notifying the  
data subject**

# Personal data breaches: ICO notification



## Which breaches?

- Must report unless breach “*unlikely to result in a risk to the rights and freedoms of persons*”
- Consider likelihood and severity of resulting risk
- Consider:
  - Type of breach
  - Nature, sensitivity and volume of personal data
  - Ease of identification of individuals
  - Severity of consequences for individuals

## When?

- Without undue delay and not later than 72 hours after becoming “aware” of breach
- If delayed, provide reasons
- Consider notification in phases

# Personal data breaches: ICO notification



## What?

- Description of nature of breach including, where possible:
  - Categories and approx. no. of individuals concerned
  - Categories and approx. no. of personal data records concerned
- Name and contact details of DPO/other contact point
- Description of likely consequences of breach
- Description of measures taken (or proposed) to deal with breach
  - Include measures to mitigate any possible adverse effects where appropriate

# Personal data breaches: internal checklist



**Recognising  
a breach**

**Response  
plan**

**Allocation of  
responsibility**

**Internal  
recording**

**Notification  
processes**



# The next two years: Covid-19 & Brexit







# The next two years



- <https://ico.org.uk/for-organisations/data-protection-and-brexit/>
- Barnier's speech on 15 May 2020 following Round 3:
  - Police and judicial co-operation a sticking point
  - Data protection approach explicitly called out
- Posturing?
- UK's adequacy in the balance?

BREXIT

COVID-19

- Changed working practices: data protection more important, particularly security
- Data protection is embedded: eg contact tracing apps
- Technology pressing ahead: smart cities; AI
- <https://newsroom.nccgroup.com/documents/ncc-group-a-blueprint-for-secure-smart-cities-whitepaper-95577>



**Ask us more questions:**

**events@cornerstonebarristers.com**

**For instructions and enquiries:**

**elliottl@cornerstonebarristers.com**

**dang@cornerstonebarristers.com**

**samc@cornerstonebarristers.com**