REGULATORY ESSENTIALS TRAINING PROGRAMME 2020: DATA PROTECTION IN FINANCIAL SERVICES – 1 JUNE 2020

Jo McLean

Managing Associate – Commercial & Data Protection

ADDLESHAW GODDARD

DATA PROTECTION 2020: KEY LEGISLATION

DATA PROTECTION LAW IN 2020

General Data Protection Regulation ("GDPR")

Provides the general framework for handling personal data in Europe

Data Protection Act 2018 ("DPA18") and **Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019**

Applies the GDPR in the UK and provides exemptions from certain rules e.g. subject access requests. Should be read in conjunction with the GDPR.

Note that the **Data Protection (Charges and Information) Regulation 2018** requires certain organisations to register with the ICO in the UK.

Privacy & Electronic Communications (EC Directive) Regulations 2003 ("PECRs")

Specific legislation for electronic marketing including email, cookies and online behavioural advertising.

This is undergoing review currently by the European authorities.

GDPR – WHY WAS IT SO SIGNIFICANT?

- Increased penalties in the UK from £500,000 to £17M (20M euros) or 4% of annual worldwide turnover (whichever is higher)
- Increased **accountability** obligations around documenting what an organisation does with data, e.g. through processing registers, and undertaking mandatory privacy impact assessments
- Enhanced **data subject rights**, e.g. removing charges to rely on rights and reducing time scales by which rights need to be complied with
- Requires organisations to be more **transparent** around the handling of personal information.

DATA PROTECTION 2020: TOP TEN TOPICS

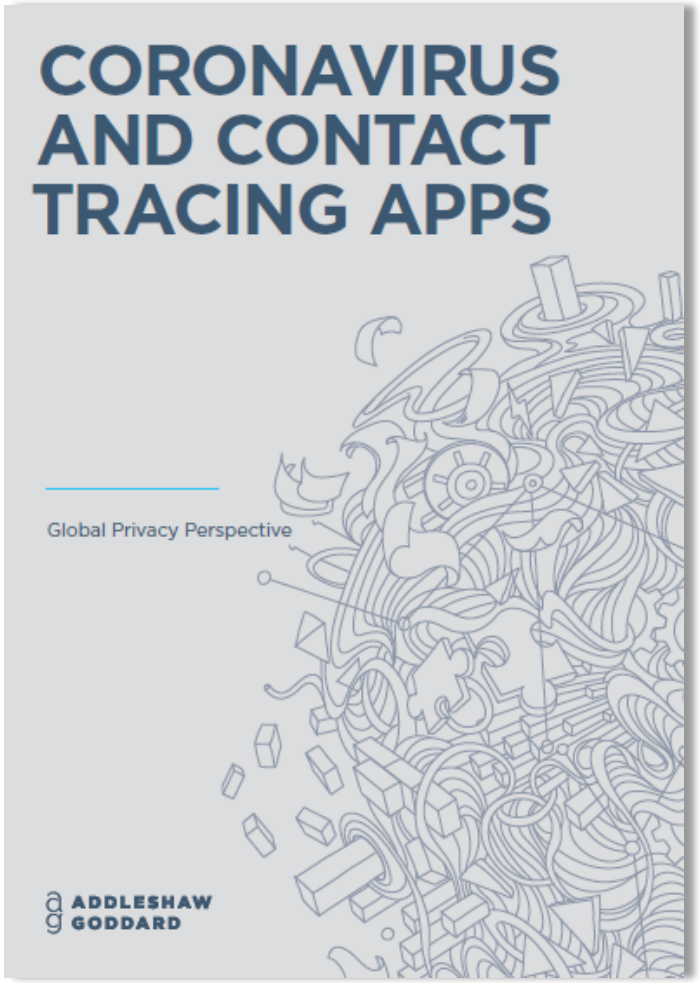
1

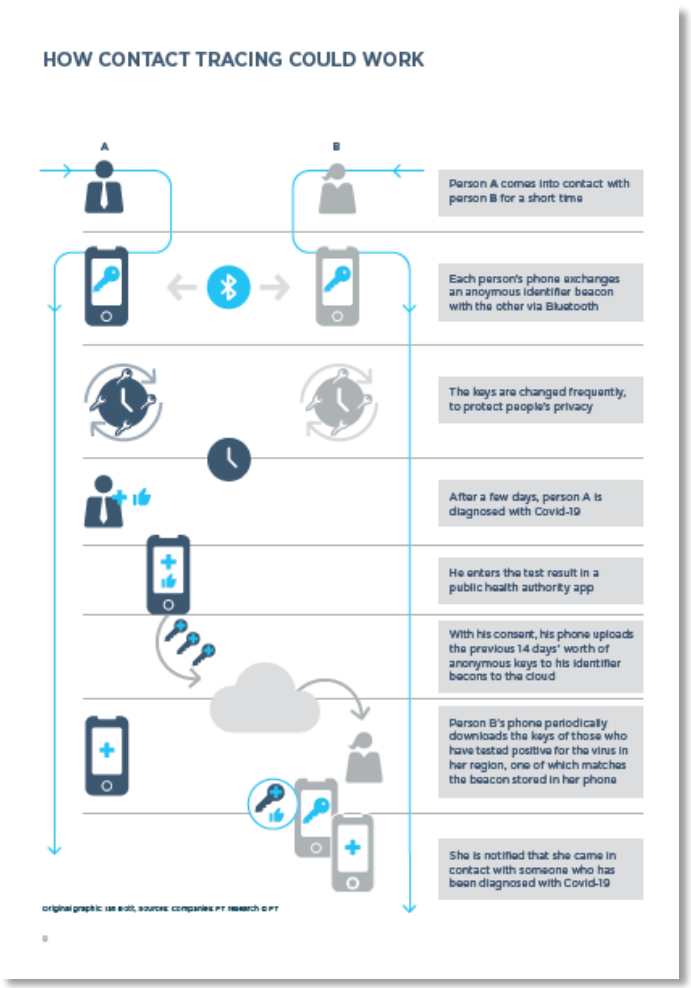
COVID-19 & DATA PROTECTION

PRIVACY HITS THE HEADLINES AGAIN

- NHSX contact tracing app has attracted a lot of attention.
- Return to work issues are involve a privacy dynamic.
- Thermal imaging and other testing involves processing of special category data.
  - Run a privacy impact assessment – template DPIA created by ICO.
  - Lawful basis?
    - Legitimate interests?
    - Employment processing condition for use of health data.
  - Consider on a role by role basis?

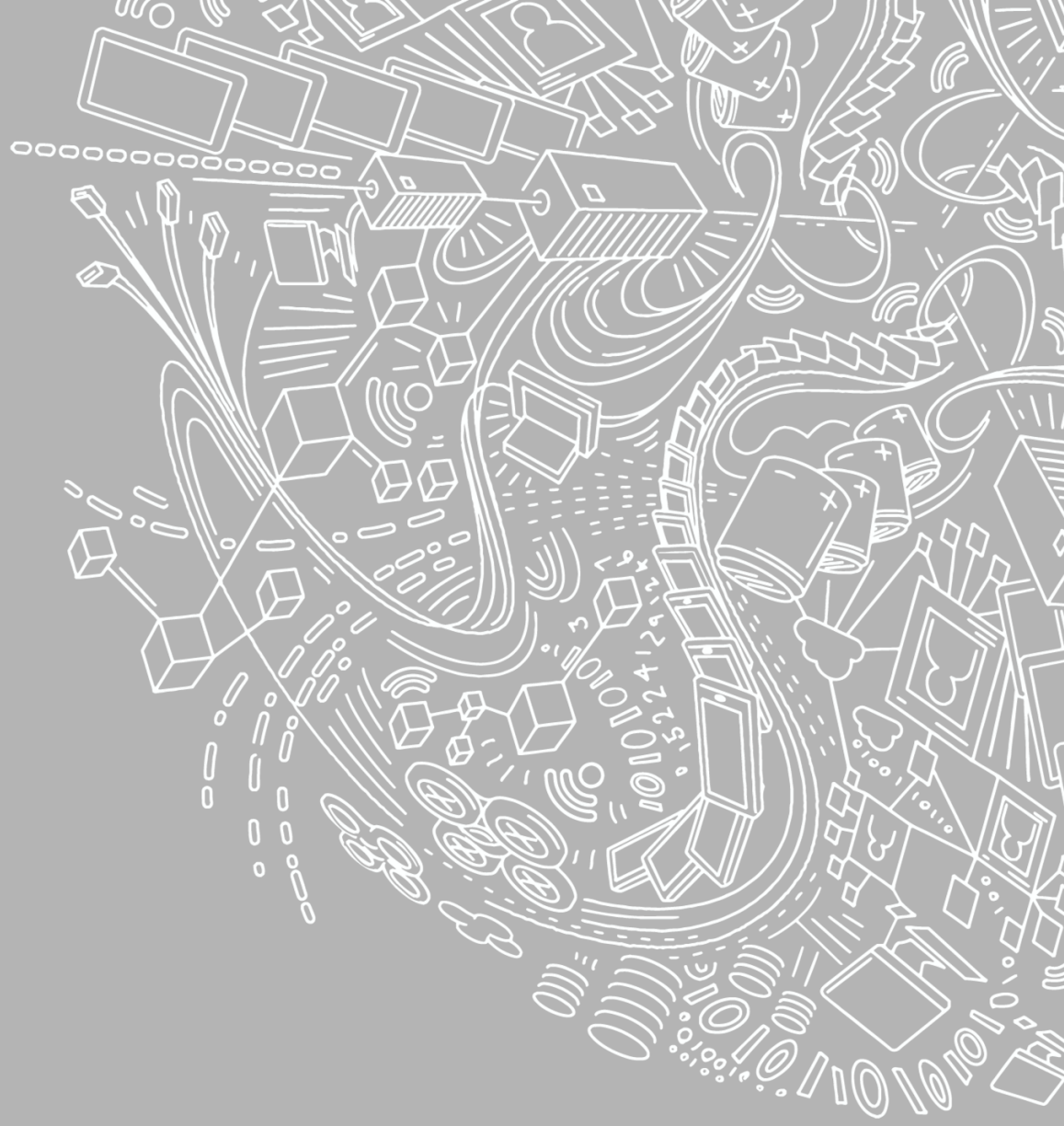
FOR MORE READING
CHECK OUT OUR WEBSITE





2

WORKING FROM HOME… THE NEW NORM?



WORKING FROM HOME & DATA PROTECTION

- Fatigue and lack of supervision is leading to data breaches.
- Reporting requirement to ICO for certain data breaches within 72 hours.
- ICO recognises delays in reporting due to Covid-19.
- Test that your current policies and procedures also can “work from home”

3 DSARS – STILL ON THE RISE

HANDLING DATA SUBJECT ACCESS REQUESTS

- 42% of all issues raised with ICO relate to DSARs. General perception that there is an increase in DSARs, triggered in case of data breach or issues in business, e.g. employment case.
- Technology / rights groups submitting DSARs on behalf of data subjects increasing. These are disappearing as fast as they are appearing.
- Claims Management Companies continuing to use DSARs to cause disruption.
- **Magnacrest** fined in criminal courts for ignoring DSAR and failing to comply with ICO Enforcement Notice.
- Follows similar action against **SCL Elections** (Cambridge Analytica).

TOP TIPS WHEN HANDLING DSARS

- Month starts when:-
  1. confirmed identity (if necessary); and
  2. clarifications received if reasonably needed to find the data.
- One month to respond:-
  - Runs from date received to next month, i.e. 3 October to 3 November – or if month shorter, the last day of the following month.
  - Weekends / public holidays – next working day.
- Can extend period by 2 months if the request is complex or you have received a number of requests from the individual.
- Can refuse if manifestly unfounded or excessive.
- Can apply exemptions in DPA 2018

4

REMEMBER BREXIT?

BREXIT ISSUES – CONTRACTUAL RE-PAPERING?

- Data transfers from European Member States to the UK will need steps taken as a result of the UK being treated as a third country.
- Latest – Department for Digital, Culture, Media & Sports issued on 13 March explanatory material to European Commission to explain the UK's data protection framework.
- EU has confirmed that they would accept "essential equivalence"
- Standard contractual clauses still needed - **EU processor** to **UK data controller** transfers under scrutiny.
- Processing activities in Europe will likely require an **authorised representative**.
- **One stop shop** issues.

5

ICO… SLOW AND STEADY…

ARE THEY TAKING THIS SERIOUSLY?

- BA and Marriot fines – still awaited – announced in **July 2019**!
- Due in August now…
- Only one fine issued by the ICO under the GDPR since 25 May 2018.
  - **Doorstep Dispensaree Ltd** fined in December 2019 where 500,000 documents containing names, addresses, dates of birth, NHS numbers and medical information and prescriptions were kept in unsealed containers. Containers were damaged in the rain.
- Compares poorly to other European regulators, e.g. Germany has issued 25+ fines, France has fined Google €50m.
- Has been a track record of bigger fines under the DPA 1998.

6

WHAT INCIDENTS HAVE THE ICO BEEN ENFORCING FOR?

ICO REGULATORY ACTION (UNDER DPA 1998)

Marketing Fines

- **Black Lion Marketing** - £171k – 27 March 2020 – Unsolicited direct marketing calls.
- **CRDNN** – £500k - 2 March 2020 – 193M automated nuisance calls.

Security Breaches

- **Cathay Pacific Airways** – £500k – 4 March 2020 – Customer database subject to brute force attack – number of errors, e.g. back ups not password protected, unpatched servers, and unsupported servers in use.
- **DSG Retail** - £500k – 9 Jan 2020 Cyber-attack on POS computer system affecting 14M.

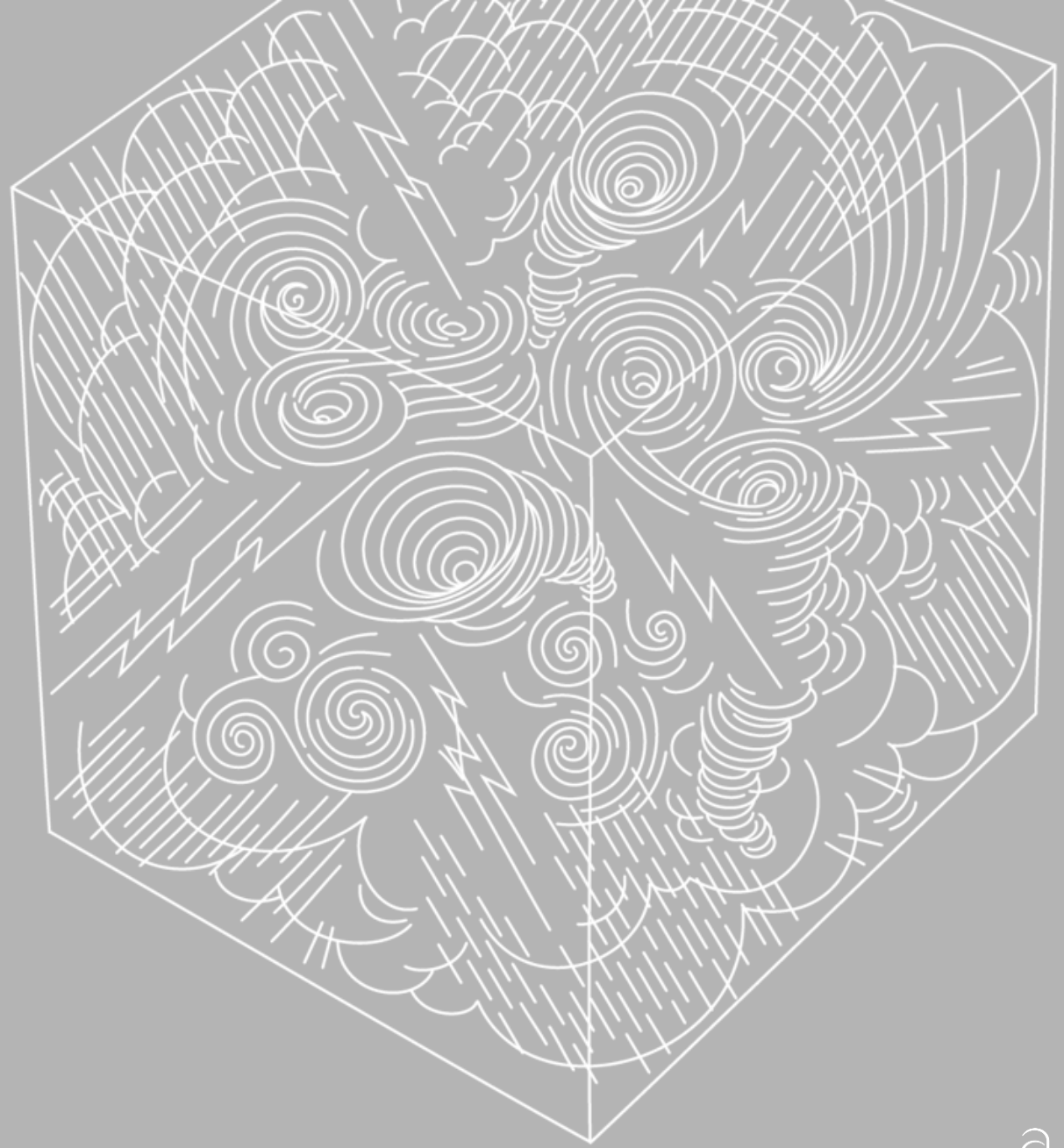
7

ICO PRIORITY AREAS TO BE MINDFUL OF

KEY AREAS FOR THE ICO IN 2020 POST COVID-19

1. **Protecting vulnerable citizens** – unlawful collected of data during crisis.
2. **Supporting economic growth and digitalisation** – giving information and support for businesses to grow and offer services safely when sharing personal data or developing AI tech.
3. **Shaping proportionate surveillance**.
4. **Enabling good practice in AI** – focussed on Covid-19 – auditing framework.
5. **Enabling transparency** – supporting organisations to be transparent to improve public confidence.
6. **Maintaining business continuity** – internal ICO focus to prepare for future.

8 CLASS ACTIONS…



IS THE TIDE TURNING?

Google v Lloyd

Subject to appeal to Supreme Court.

Morrisons

Supreme Court overturned decision **but** doesn't rule out future similar actions.

Equifax

Class Action Withdrawn but Opt-in Group Litigation Action against BA ongoing.

9

WHAT DOES THIS MEAN FOR LIABILITIES?

WHERE ARE WE GOING?

Uncapped Liability

Super caps of £20M and up and separate cap

Multiples of spend and separate cap

Now much more complex…

FACTORS TO THINK ABOUT

Indemnities & Caps

Do you need the indemnity?

What is the per annum spend?

Would that work as a multiple? Floor? Paid and payable?

How many records are being processed?

Use a standard scale (IBM / Poneman - $150 per record)

What is recoverable?

Some could be uncapped, e.g. cost of giving credit reference searches.

Insurance in place?

Might enable a higher cap but heads of claim are tricky.

10

DPO ROLE IN FOCUS

DPO AND CONFLICT OF INTEREST – AREA OF GREATER SCRUTINY

- Belgium decision has called into question the role of a DPO when shared with other roles.
- Fined **Proximus** SA 50,000 euros because it was impossible for the DPO to exercise independence when overseeing his other responsibilities where he was head of compliance and audit and risk – infringing Article 38.6 of the GDPR.
- What does this mean?
  - Questionable decision given guidance flags that holding a dual role hasn't been ruled out.
  - Emphasis will be on protocols to manage conflicts and what the role is shared.
  - What about due diligence on suppliers?

ANY QUESTIONS?

CONTACT US

JO MCLEAN
Managing Associate
+44 (0)131 222 9541
+44(0)7501 463 230
jo.mclean@addleshawgoddard.com

www.addleshawgoddard.com

Aberdeen, Doha, Dubai, Edinburgh, Glasgow, Hamburg, Hong Kong,
Leeds, London, Manchester, Muscat, Singapore and Tokyo*

* a formal alliance with Hashidate Law Office