

GDPR compliance – a risky business?

Eleanor Tunncliffe
Legal director

eleanor.tunncliffe@hildickinson.com
0113 487 7978

Programme

- Case studies – what goes wrong?
- New obligations
- New risks
- Q&A

Could it be you?

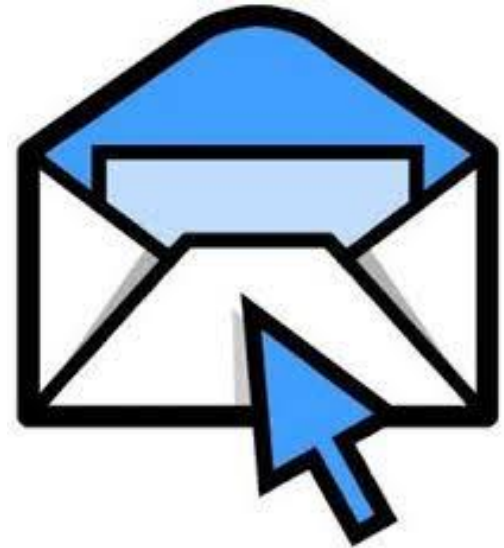


Soho sexual health clinic - £180,000 fine

£180,000 fine

The clinic provides HIV services and sends a regular newsletter to its patients by email. One month the recipients were “cc’d” rather than “bcc’d”. All the recipients could see one another’s addresses. 730 of the email addresses contained people’s full name.

Breach = failure to have appropriate technical security measures in place re sending the newsletter



Regal Chambers Surgery - £32,000 fine

£32,000 fine

A child's parents were going through an acrimonious divorce. Despite being aware of this, the surgery disclosed information from the child's medical records to his father, which contained sensitive information – including confidential contact information – about the child's mother.

Breach = failure to have a policy for handling subject access requests



Bayswater Medical Centre - £35,000 fine

£35,000 fine for failure to secure data in
unoccupied premises

Breaches =

- Medical records stored in unlocked cabinets
- Medical records left on windowsill in view of the street
- Repeat prescriptions left on view in the office
- Patient identifiable information not securely destroyed



Whitehead nursing home - £15,000 fine

An employee of the nursing home regularly took her laptop home to complete unfinished work. One night her home was burgled and the laptop was stolen.

The laptop held confidential information about patients and staff. It was not encrypted.

Breaches =

- **failure to encrypt laptop**
- **failure to have home working and encryption policies in place**
- **failure to provide staff training**



Data protection risks – what's new?

1

- New GDPR obligations, especially the duty to demonstrate compliance

2

- Greater public awareness of data protection rights and obligations
- Easier to bring claims

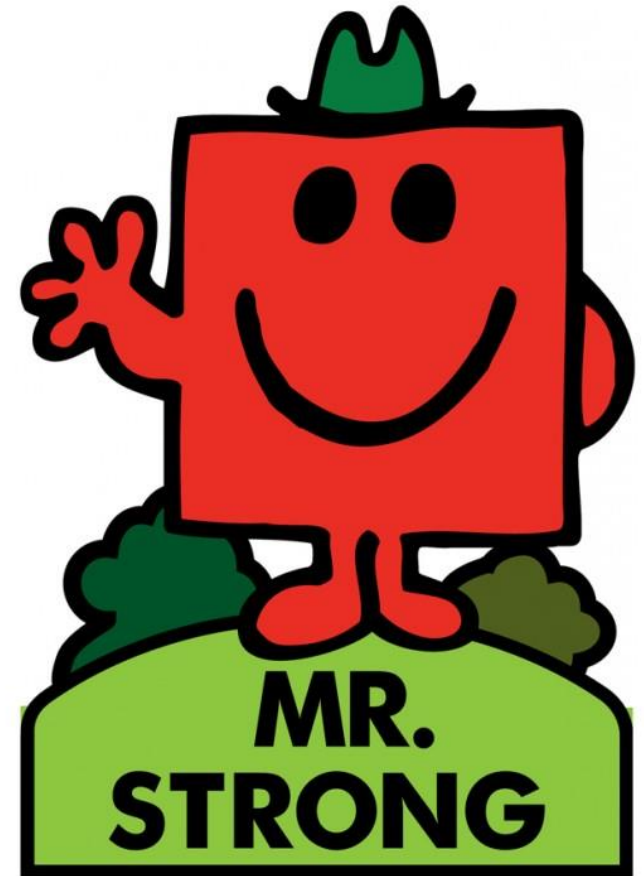
3

- Maximum fines are increasing from £500k to €20m

New GDPR obligations

What's new?

- Duty of **accountability**
- **More information provided to data subjects**
- Amended conditions for **data sharing**
- Stricter rules about **consent**
- Lots of new **data subject rights**
- New rules for **data processing agreements**
- **Data Protection Officers**
- Focus on **data retention and deletion**



More information for individuals

Privacy notices

Need to tell people that you are processing their personal data and what you are doing with it.

New prescriptive (and long!) list of what should be included.

Will need different notices for the different types of people whose personal data you use:

- Patients
- Next of kin
- Staff (employees, independent contractors)
- Non-exec directors, governors
- Members of the public on your premises (CCTV, ANPR)
- People who use your website



Make sure you have identified all of the types of people that you process personal data about.

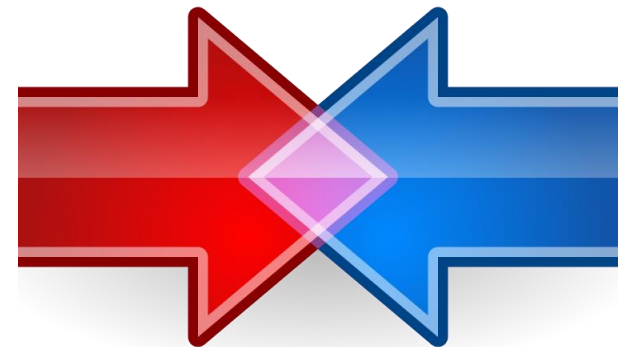
Privacy notices

If you are using personal data about children you will need to have a notice worded for them



TAKE CARE!

If you are working with another organisation to decide what information is collected or how it is stored you may be **joint data controllers**. You will need to let people know about the data protection arrangements between the joint controllers



Data sharing

Data sharing



DPA 2018 condition (health data)

Article 9 GDPR condition (health data)

Article 6 GDPR condition



Conditions for processing – Article 6

- a) Consent
- b) Necessary for performance of a contract
- c) Compliance with legal obligations
- d) Vital interests
- e) Task carried out in the public interest or in exercise of official authority
- f) Legitimate interests **TAKE CARE! No longer applies to public authorities**



Conditions for processing – Article 9

- a) Explicit consent;
- b) Vital interests;
- c) Charity or not-for profit bodies;
- d) Manifestly made public by data subject;
- e) Legal claims;
- f) Substantial public interest;
- g) Health and social care;
- h) Public health;
- i) Historical, statistical or scientific purposes.

Sometimes the DPA 2018 imposes extra conditions



Consent

MYTH: To comply with the GDPR I need people's consent to process their personal data

Normally you will not need to rely on consent as there will be another GDPR condition you can use instead



Consent



There are now strict rules about what counts as consent – it must be explicit

TAKE CARE!

The rules about consent under the GDPR only apply if you are relying on the GDPR consent condition

They do not affect:

- Law of consent to care and treatment
- Consent to participate in research
- Ability to rely on implied consent as the basis for sharing information for direct care, to avoid breaching the law of confidentiality (as established under *Caldicott* reviews)

Data Controllers and Processors

Data controllers and processors

- Need to carry out due diligence carried out on data processors and any sub-processors.
- There must be a binding agreement between the controller and the processor
- Contract must include minimum terms

Examples of typical data processors:

- IT suppliers (Microsoft, Apple)
- Telephony suppliers
- Hosting services
- Pay roll services
- Data analytics

TAKE CARE!

Some contracts for data processing services are held centrally by DHSC/ NHSE. Make sure you are legally able to enforce their terms.

Data controllers and processors

Description of the subject matter and duration of the processing	Description of the nature and purpose of processing	Description of the type of personal data and categories of data subject	Description of the rights of the data controller	Process only on documented instructions from controller
DP staff are subject to duty of confidentiality	DP ensures security of processing (Article 32)	Controller consent required to sub-contract	Sub-contracting agreement to replicate DP agreement	Assists controller to comply with data subject rights
Assists controller with notification of data breaches	Assists controller with data protection impact assessments	Deletion or return of personal data at request of controller	Assists controller to demonstrate compliance with GDPR	

Data controllers and processors – some tips

See the Crown Commercial Services Policy Procurement note for standard contract terms and guidance on procurement.

Make sure that due diligence procedures will be followed regardless of the value of the services. Build into procurement process.

Make sure due diligence is carried out on proposed sub-contractors. Avoid “hard-wiring” approval of sub-contractors into the contract where possible.

Keep a central log of data processing agreements



Data Protection Officers

Data Protection Officer

- Reports to highest level of management
- Must be able to act independently
- May be one DPO for a number of organisations – can contract out
- Take care with conflicts of interest – DPO shouldn't mark their own homework!



Accountability

Accountability



Risks

MYTH: We could be fined £millions for a technical breach of the GDPR

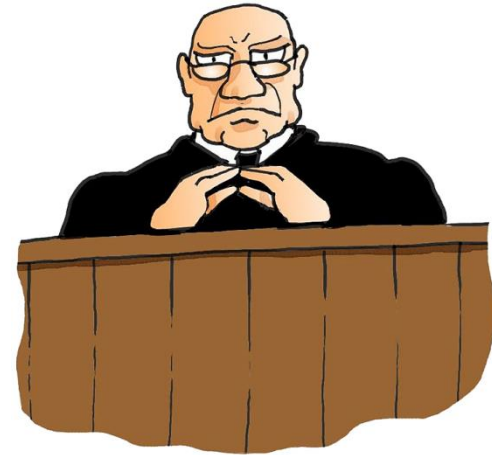
In practice this is very unlikely to happen as it would not be a proportionate use of the ICO's power to fine. It would also be very much out of step with the ICO's approach to fines to date.



The NHS already has a process for breach reporting:
***Guide to the Notification of Data Security and Protection
Incidents post GDPR and NIS Directive (NHS Digital 2018)***

What if I don't comply?

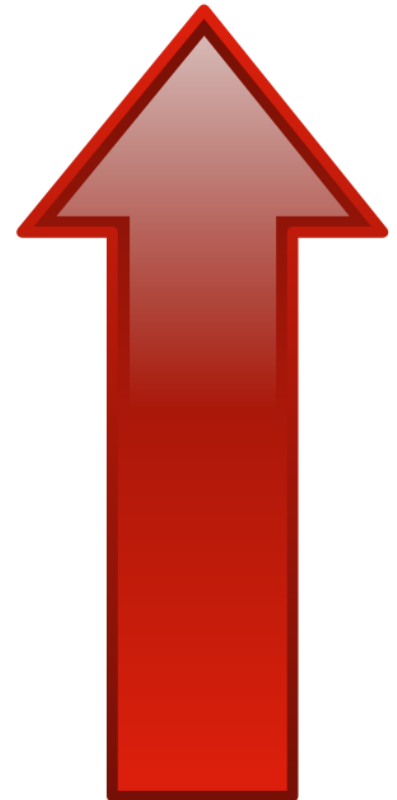
- Maximum fine is now €20 million
- Clear that data subjects can bring claims for damage and/or distress.
- Controllers have joint and several liability with other data processors and controllers involved in the processing
- Reputational risk



Make sure your agreements give you scope to clawback any damages you have to pay out due to someone else's error.

Increased likelihood of risks materialising


- Greater awareness among the public of data protection obligations:
 - Publicity given to GDPR in the media
 - More privacy notices being provided and more detail being given about how data is used
 - Requirement to include detail of rights to appeal to the ICO in privacy notices and when responding to requests
 - General requirement to inform the ICO and individuals of breaches
- Easier to claim:
 - Clear that “damage” is not required to bring a claim
 - If more than one organisation is involved, don’t have to identify which one is at fault



Plus ca change?

- Data security still very likely to be the area that prompts most regulatory activity
- Despite the increased focus on cyber security, most breaches are “old school” breaches rather than hacks
- Staff training still key

BUT new areas of attention are likely to include:

- Privacy notices
 - Data retention
 - Data processing agreements and due diligence
 - New data processor responsibilities
- 

MR. WORRY

by Roger Hargreaves



Er, so what if I haven't done all of that?

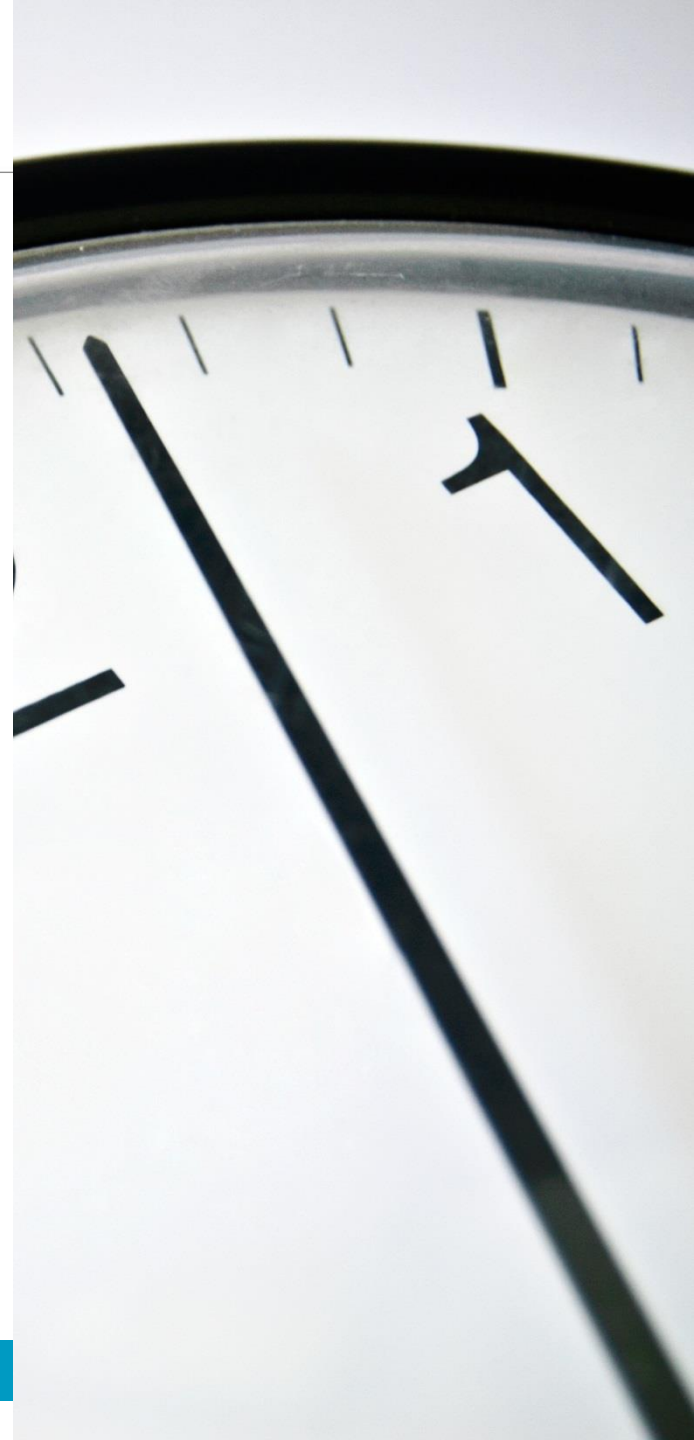
Getting up-to-date

If you know that you are not up to speed on a GDPR requirement, keep a record of this and your plans for sorting it out.

Things to focus on are:

- Appointing a DPO if you need one
- Your record of processing activities
- Your fair processing notices
- Raising awareness of GDPR among staff through training, in particular about security and data subject rights

Many materials can be shared between organisations



Useful resources

There are useful documents and guidance on the ICO website www.ico.org.uk. See in particular:

- Producing a record of processing (including template) <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/documentation/how-do-we-document-our-processing-activities/>
- General guide to the GDPR <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/>
- EU checklist for DPIAs (see Annex 2) http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236



Questions?

Eleanor Tunnicliffe
Legal Director

0113 487 7978

Eleanor.tunnicliffe@hilledickinson.com

Eleanor acts primarily for the public sector and advises healthcare organisations in relation to a variety of issues, with a particular emphasis on public law, judicial review, primary care commissioning, disputes between healthcare commissioners and providers and information governance.



A presentation by

HILL DICKINSON

