first response

DMH Stallard

Part two – third parties and your supply chain

Act now to protect your business assets

Contents

Protecting your business assets

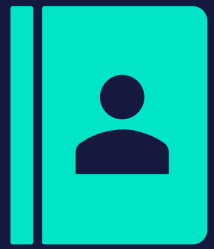
Debbie Venn, DMH Stallard

In this session …

- Internal processes:
  - Consider what you have in place (eg, policies on handling personal data, confidential information, trade secrets (for internal handling)
  - What external contracts or NDAs are in place?
- Overview of legal requirements:
  - GDPRs / DPA obligations
  - ICO / timeline and process
  - Notifications: insurers, ICO and data subjects
- Practical considerations
- Confidential information and commercially sensitive information – additional legal obligations attached under contracts or law, as well as Usage Policy for such information
- Personal data – statutory obligations

Overview of legal requirements – personal data

- GDPRs / Data Protection Act 2018 (“DPA”)
  - Themes:
    - Protecting data subject’s rights, especially protection of data relating to children
    - Businesses need to demonstrate compliance
  - Data protection principles:
    - Lawful, fair and transparent
    - Purpose limitation and data minimisation
    - Accuracy
    - Storage limitation (retention periods)
    - Integrity and confidentiality
    - Accountability



Key data consideration for cyber security

- Personal data: includes anything that identifies a living individual, such as names, addresses, email addresses of clients

- Special category data: includes medical records, religion, political opinions, biometric data. There are additional obligations apply to processing special category data

- Processing: obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data

- Technical and organisational measures: Key for assessing security - ***The Sixth Principle*** - *data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised loss, destruction or damage, using appropriate technical and organisational measures.*

Non-compliance implications

- Fines (for breach of UK GDPRs) up to:
  - Tier 1 – the higher of **£8,700,000** or 2% of gross global turnover (non-compliance)
  - Tier 2 – the higher of **£17,500,000** or 4% of gross global turnover (breach)
- Legal actions, including claims for breach of contract or other losses
- Reputational damage to brand / bad publicity
- Disgruntled customers and employees
- Criminal proceedings
- Data subjects – right to compensation (Article 82)
- Audit and Enforcement Notices from the ICO

Data breach notifications under GDPRs

- You need to analyse the breach ASAP and try to minimise damage and any further breach
- Data security breach has to be notified to the ICO if the security breach is one that leads to the accidental and unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data
- Timing of notification:
  - Data controller – notify ICO within 72 hours from receipt of notification of data breach
  - Data processor – notify data controller without undue delay from receipt of notification of data breach (not obliged to notify the ICO)
  - Data processing agreements – advisable to agree a reportable time period when you are the data controller, to put breach plan into action at the earliest opportunity
- Failure to notify of a data security breach is a breach of the GDPRs itself, therefore notify within the 72 hour window, even with limited information
- Failure to notify in accordance with a data processing agreement / DP provisions, could be breach of contract

Compensation to data subjects

- Personal data breaches need to be notified to data subjects where there is a high risk to a data subject's rights, without undue delay
- No need to notify if:
  - Technical organisational measures render personal data unintelligible, ie, encrypted
  - DC takes steps to ensure personal data is no longer subject to high risk
  - Notifying data subjects requires disproportionate effort
- Notices to data subjects must include: (i) description of security breach in plain language; (ii) contact information for enquiries; (iii) details of likely consequences of security breach and mitigation steps taken
- Right to compensation where data subject has suffered material or non-material damage
- A controller or processor will not be liable to pay compensation where they can prove they are not in any way responsible for the breach event
- No guidance on amounts – this would be determined by the UK courts

Data breach policy and process

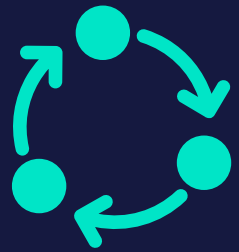
- Takes pressure off in the event of a breach in determining who needs to be involved, notifications, etc, when the event happens
- Ensures compliance with legal requirements and helps support technical measures
- May help mitigate liability with the ICO (and potentially reduce fines) and reduce risks attached to a data breach (eg, compensation payable to data subjects)
- Policy should cover:
  - Escalation process and response plan, including key contact details
  - Notification timeframes
  - Third parties involved, eg, legal, PR, forensics
  - Process for informing data subjects and dealing with data subject compensation, press releases, etc
  - Notification to insurers?
  - Review and update, to ensure technical and organisational measures are up-to-date and align with current processes

Technical and organisational measures – what to do

- Pseudonymisation and encryption of personal data
- Ensure the confidentiality, integrity, availability and resilience of processing systems and services (eg, passwords, regular update of software and firewall, anti-virus, anti-malware)
- Ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident (eg, regular backup)
- Regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing
- Restrict staff access to personal data to those who need to know – help minimise risk
- Ensure physical security on premises (eg, policy for staff to lock away their documents overnight in secure cabinets, and destroy any sensitive printouts)
- Put in place a BYOD (bring your own device policy) and Data / Information Usage Policy
- Implement a strict ban on the use of personal email for work purposes

Key things to consider for storing / sharing data

- Audit your systems and identify areas of vulnerability to put further protective (technical and organisational) measures in place – review and update
- Ensure you have contracts in place with third parties who process data/business information and have appropriate processing provisions, including escalation process
- Vetting and training of staff, contractors, vendors and suppliers on continuous basis on data obligations and cyber issues, to identify risks and reduce human error
- Data Breach Policy – put one in place to manage a data breach, including escalation procedure, together with documented process / template responses – test and update!
- Discuss with insurers to get right cyber security policy / cover
- If a breach occurs:
  - ACT QUICKLY TO PREVENT FURTHER DAMAGE!
  - Notify as required to ICO and data subjects and manage comms
- Learn from experience and update policy and procedures



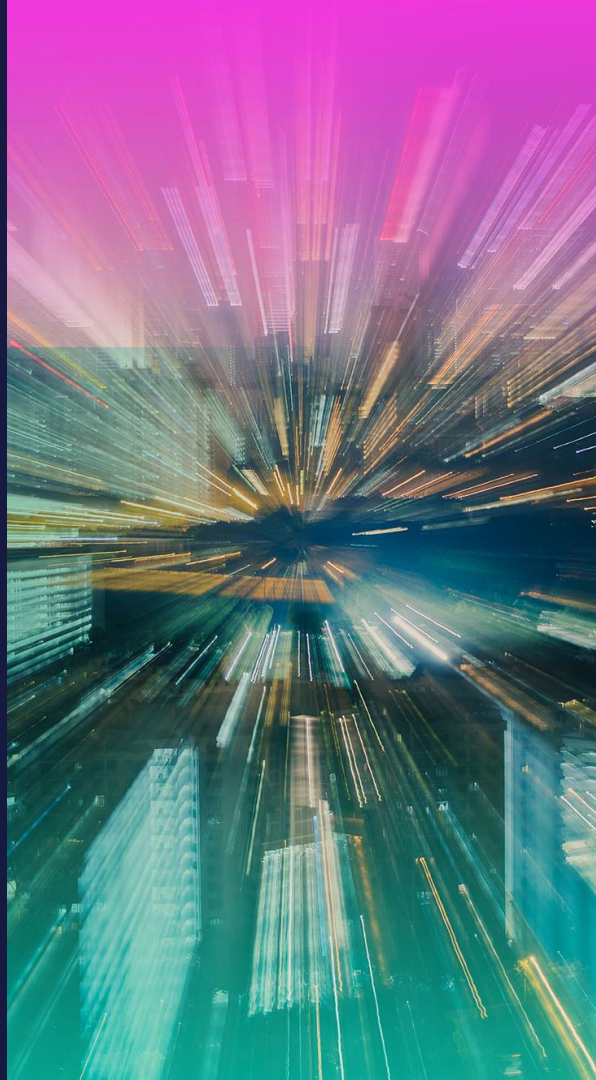
first response DMH Stallard

What happens if it all goes wrong?

Nicola Billen, DMH Stallard

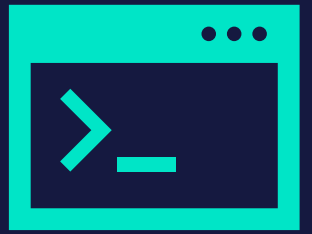
What remedies are available?

- Breach of UK GDPR
- Misuse of private information
- Breach of confidence
- Negligence



Warren v DSG Retail Limited [2021] EWHC 2168 (QB)

- Cyber attack, personal data compromised
- C brought a claim for breach of DPA 1998, misuse of private information, breach of confidence, negligence
- Dixons - Summary Judgment / strike out of all causes of action save for DP principles
- Claim for misuse / breach of confidence – must be “use” or “misuse”
- Claim for negligence – failed



Stadler v Currys Group Limited [2021] EWHC 3809 (QB)

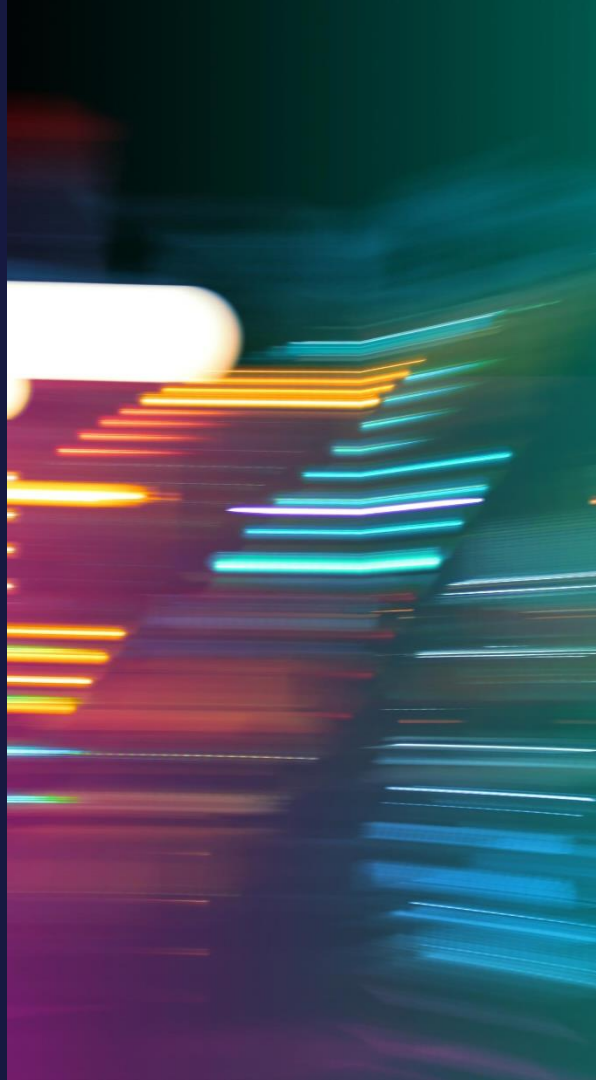
- C bought a smart TV – defective
- D sold on for repair and resale
- No data wipe / factory reset – Cs account used to buy a movie
- Claim for breach of UK GDPR, misuse of private information and breach of confidence
- Damages for distress

Cleary v Marsten (Holdings) Limited [2021] EWHC 3809 (QB)

- Letter for C was inadvertently sent to a colleague
- Breach of data protection legislation, breach of confidence, misuse of private information
- Sought damages
- D – one off human error and colleague did not read it
- CFA , ATE – costs to trial circa £50,000
- High Court, not County Court
- No – routine data protection claim, essentially same claim – duplication
- Small Claims Track and County Court can deliver access to justice – protection from costs and award of fair and reasonable sum

What does this mean for you as a business?

- Do not ignore your obligations, including DPA and UK GDPR
- Risk management is key – before / after the event
- Be mindful of how a breach might be perceived
- Get the experts on board



Data breach & IR preparation

John Douglas, First Response

Are you genuinely prepared for a data loss event?

- Ransomware increased 340% from 2019 -> 2022*
- Over 2,000 data loss events reported to ICO per quarter
- 40% of UK small businesses have no plans in place
  - Outsource IT to non-security aware providers
  - Have no idea what critical assets they have or where they are
  - No risk assessment, not considered what they would do
  - Don’t have acceptable use policies in place
  - Haven’t trained their users
  - Don’t keep systems patched
  - May not have viable backups
  - Don’t know who to call

Data from: https://ico.org.uk/action-weve-taken/data-security-incident-trends/

Response plans and the preservation of data

(not a Harry Potter book!)

- Secure the stolen data & relevant logs/systems
- Conduct an investigation
- Notify relevant parties
- Communicate with affected parties
- Take legal action
- Review and update policies
- Review employee training

Five lessons from data breaches in 2022

1. Importance of Regular Security Reviews
2. How third-party security is critical
3. Human error still a major problem
4. Insider threats are increasing
5. Importance of continual monitoring

Conclusion:
most organisations are not well prepared – no reason to think 2023 will be any different ☹

What we typically find

- No IR plan – minimal DR capability (better after covid)
- Have tried to handle the incident in-house
- IT have failed to preserve logs – more focussed on BAU
- Finally call us in – we discover data loss started much earlier and on-going…
- Management looking to minimise reputational harm, so not reporting to
  - ICO
  - Stakeholders
- Event takes longer to contain, results in significant losses

Questions

Speakers

Debbie Venn

Partner, Commercial
DMH Stallard
Debbie.Venn@dmhstallard.com

Nicola Billen

Partner, Despite Resolution
DMH Stallard
Nicola.Billen@dmhstallard.com

John Douglas

Technical Director
First Response
John.Douglas@first-response.co.uk