

Lifecycle of a data breach: how to identify, respond to and learn from breaches.

Advocate Davida Blackmore, Callington Chambers

Samantha Gardner, Office of the Information Commissioner

Dave Cartwright, Grant Thornton

CALLINGTON
CHAMBERS



Topics

- Definition of a “personal data breach”
- What does a data breach look like?
- Lifecycle of a breach
- Case studies (interactive session)



Definition of a data breach



DATA PROTECTION (JERSEY) LAW 2018

“personal data breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed” (Art.1)

“Personal data means any data relating to a data subject” (Art.2(1))

Why does this matter?

- Recital 85 of the GDPR states that

"A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned"

Not all breaches are created equal



Not me, surely?

APPLEBY

Butlin's

FIFA[®]

For the Game. For the World.

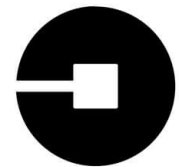


 **Marriott.**


CATHAY PACIFIC



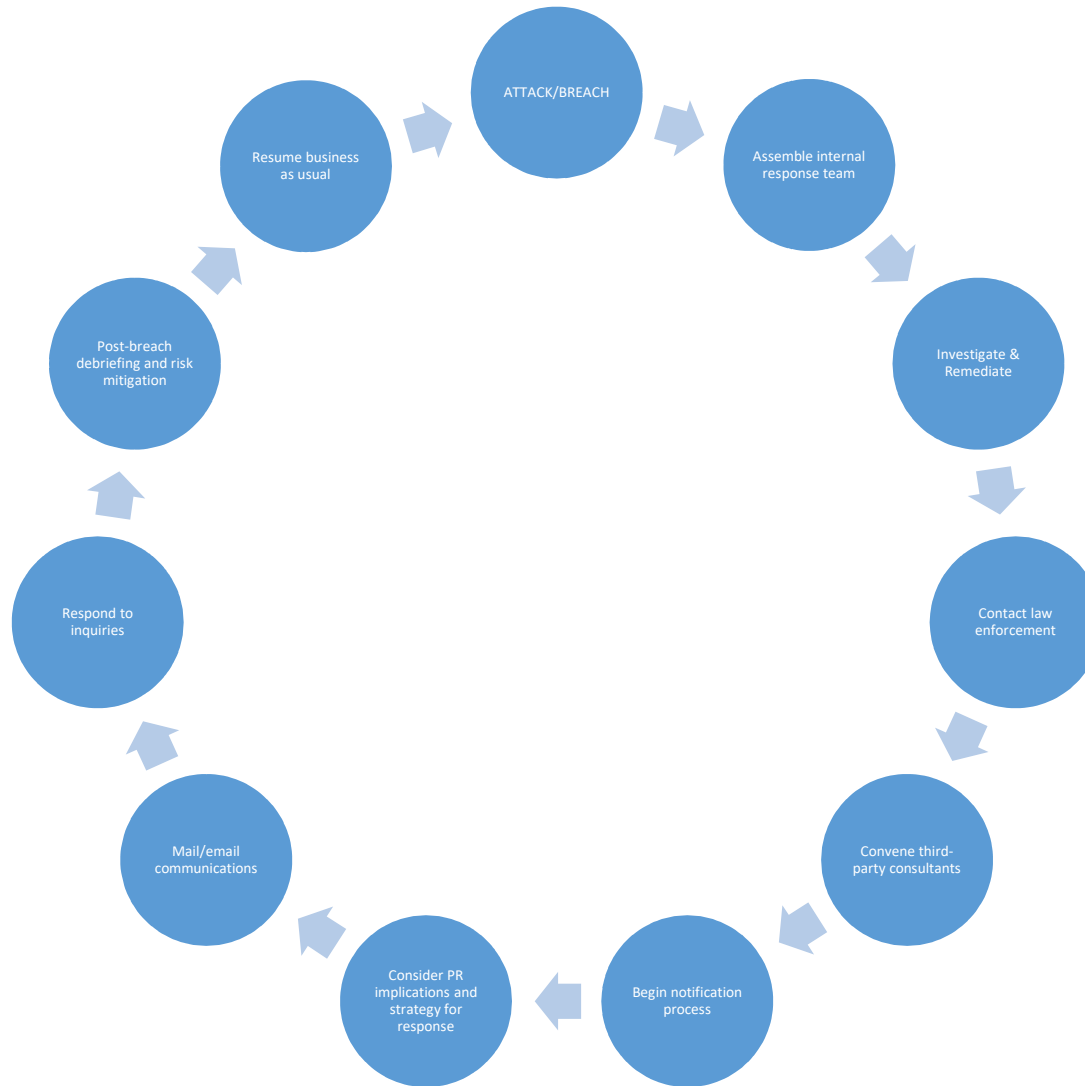
UNDER ARMOUR



UBER



Lifecycle



Attack/breach

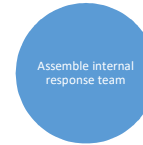


206

\$5.99m

\$8.70m

Assemble internal response team



- Policies and procedures
 - Define trigger events
 - Train staff:
 - Provide examples of what to look for and how to respond
 - Make sure that they know how to identify different types of breaches e.g. theft/loss, hacking, employee snooping, malware
 - Do's and Don'ts
- Key individuals
 - IT
 - Data protection officer
 - Management
 - Comms

Data breach plan

- What a data breach is and how staff can identify one
- Clear escalation procedures and reporting lines for suspected data breaches
- Members of the data breach response team, including roles, reporting lines and responsibilities
- Details of any external expertise that should be engaged in particular circumstances
- How the plan will apply to various types of data breaches and varying risk profiles with consideration of possible remedial actions
- An approach for conducting assessments
- Processes that outline when and how individuals are notified
- Circumstances in which law enforcement, regulators (such as the OIC), or other entities may need to be contacted
- Processes for responding to incidents that involve another entity
- A record-keeping policy to ensure that breaches are documented
- Requirements under agreements with third parties such as insurance policies or service agreements
- A strategy identifying and addressing any weaknesses in data handling that contributed to the breach
- Regular reviewing and testing of the plan
- A system for a post-breach review and assessment of the data breach response and the effectiveness of the data breach response plan

Investigate/remediate



- Assess the nature and scope of the breach
 - Identify what systems and types of information (including any special category data) have been accessed or misused
 - Number of data subjects
 - Number of records
- Work out risk exposure
- Plan appropriate response determination
- Art.20(5) of the DPJL requires data controllers to keep a log of ANY Breach:
“The controller must document any personal data breaches, including the facts relating to the personal data breach, its effects and the remedial action taken, in such detail as will enable the Authority to verify its compliance with this Article.”

Who you gonna call?

Contact law enforcement

- JOIC for guidance
- Police
- Insurer
- JFSC
- Media relations
- Lawyer
- External security consultants



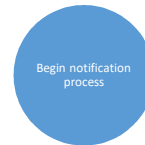
Credit: Columbia Pictures

Convene third-party consultants



- Incident response is a subject in its own right
- The initial response has to be internal
 - Large company may have a trained internal response team
 - Small companies can be really basic – a small group and a plan of whom to call
- Some will be directly related to responding to the breach
 - Techies, digital forensics, cyber specialists, etc.
- Some won't
 - PR advisors, legal advisors

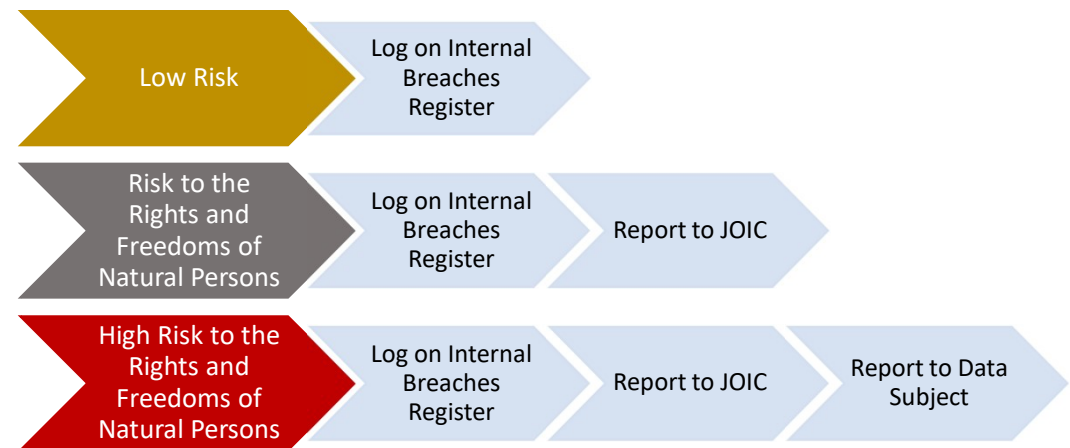
Begin notification process



- Processors must notify their controller of ANY breach (Art.22(1)(g))
- JFSC
- Information Commissioner

“In the case of a personal data breach, the controller must, without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach in writing to the Authority in the manner required by the Authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.”
(Art.20(1))

- Data subjects



Home > Data Protection (New Law)

Data Protection (New Law)

The Data Protection (Jersey) Law 2018 and the Data Protection Authority (Jersey) Law 2018 came into effect on 25 May 2018. This page includes guidance, the new legislation (including EU legislation), resources, infographics and useful links to other websites to assist organisations in working towards compliance. More information will be added as it becomes available.

Please click on the sections below to view more:

GUIDANCE

RESOURCES

- [Guidance for States Members](#)
- [Guidance on Transitional Provisions](#)
- [The Data Protection Principles](#)
- [Key Definitions](#)
- [Guidance for SMEs](#)
- [Guidance on Breach Reporting](#)

<https://www.oicjersey.org/>

What do I need to include in my initial notification?

As a minimum:

- The name of the data controller
- The name and contact details of the DPO or other point of contact where more information can be obtained
- Whether it is a first or subsequent notification
- The date and time of the Breach (or best estimate)
- The date and time of the controller becoming aware of the Breach
- The nature and content of the personal data concerned
- Technical and organisational measures applied (or that will be applied) to the affected personal data
- The name of the organisation affected by the data breach (if different from the data controller)

What do I need to include in any follow-up?

- A summary of the incident that caused the Breach, including the physical location of the Breach
- The number and category of data subjects concerned
- The number and category of personal data records concerned
- The likely consequences of the personal data breach and potential adverse effects on the data subjects
- The technical and organisational measures taken or proposed to be taken to mitigate those potential adverse effects
- The content of any notification provided to affected data subjects
- The means of communication used to notify the affected data subjects
- The number of data subjects notified
- Whether the Breach affects data subjects in any jurisdiction other than Jersey
- Details relating the notification with any other data protection authorities
- If these details cannot be included in any second notification, a reasoned justification for the further delay

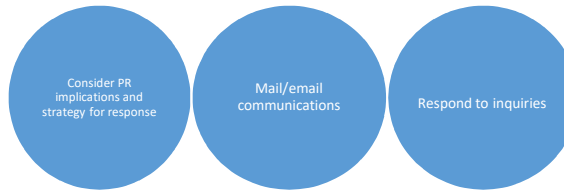
“Becoming aware” ...

- Art.29 Working Party guidelines

“WP29 considers that a controller should be regarded as having become “aware” when that controller has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised.”


http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49827

Communications




- Data subjects affected by the breach
 - Embarrassment or inconvenience is not an excuse to forgo notification
- What information should you be giving?
- Any notification to data subjects must include the following information :
 - The name and contact details of the DPO or other contact point where more information can be obtained
 - A summary of the likely consequences of the Breach
 - A description of the measures taken or proposed to be taken by the data controller to address the Breach
 - A description of the measures a data subject could take to mitigate any possible adverse effects of the Breach

Post-breach debriefing and risk mitigation



Post-breach
debriefing and risk
mitigation

Resume business as usual



Resume business
as usual

- Review
 - Policies and procedures
 - Risk assessments (DPIAs)
 - Suitability of external providers/insurance
 - Technologies
- Amend as necessary
- De-brief staff and provide further training if necessary

In summary

- **CONTAIN** the data breach to prevent any further compromise of personal information.
- **ASSESS** the data breach by gathering the facts and evaluating the risks, including potential harm to affected individuals and, where possible, take action to remediate any risk of harm.
- **NOTIFY** individuals and the Commissioner if required.
- **REVIEW** the incident and consider what actions can be taken to prevent future breaches.
- **PLAN** for the worst happening before it actually does.

Case study 1

- Employee made a subject access request
- Steps taken to retrieve and collate relevant information. Scanned on system and hard copy made ready.
- Hard copy and scanned version altered by persons unknown.
- Report to the Board by DPO following investigation and remediation. Concludes matter should be reported to relevant local data protection authority.
- Board commissions a further investigation by senior member of staff and without DPO input. Comes to a different conclusion regarding notification.
- DPO removed from post.

Case study 2

- The data, my friend, was blowin' in the wind



Case study 3

- Good old email, but with a twist
 - Auto-complete: 22% of issues reported to the OIC
 - So it's nice to have a different mail issue for a change
 - Right address, right covering note ...
 - ... and the wrong attachment



Scan_17071970.pdf

Case study 4

- Attempt to comply with data protection law gone wrong ...
 - Medical authority identified hundreds of medical files passed their retention period
 - To save time and money, they decided to burn the files via a bonfire on the beach and left it there ...
 - There was a fire ban at the time, fire brigade came along and put out the fire
 - Whilst doing so, half burnt pieces of paper were distributed all over the beach and into the sea
 - This resulted in patient personal data being viewed by many members of the public

Examples

1. Loss of a USB key with unencrypted personal data. Unclear as to whether or not unauthorised individuals accessed data.
 2. A third party informs a controller that they have accidentally received the personal data of one of its customers and provides evidence of the unauthorised disclosure
 3. A controller detects that there has been a possible intrusion into its network. The controller checks its systems to establish whether personal data held on that system has been compromised and confirms this is the case.
 4. A cybercriminal contacts the controller after having hacked its system in order to ask for a ransom.
1. Reasonable degree of certainty that an availability breach has occurred; the controller would become “aware” when it realised the USB key had been lost.
 2. As the controller has been presented with clear evidence of a confidentiality breach then there can be no doubt that it has become “aware”.
 3. Controller now has clear evidence of a breach there can be no doubt that it has become “aware”.
 4. In that case, after checking its system to confirm it has been attacked the controller has clear evidence that a breach has occurred and there is no doubt that it has become aware.

Thank you!

Advocate Davida Blackmore, Partner
davida.blackmore@callingtonchambers.com
01534 510250

CALLINGTON
CHAMBERS

Samantha Gardner, Case Worker
s.gardner@oicjersey.org
01534 716530



Dave Cartwright, Senior Consultant, Information Security
David.Cartwright@gt-ci.com
07700 898590

