GemTALK - Data Breach 101

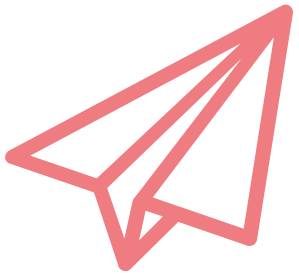
An examination into data breach procedures, responsibilities and reporting mechanisms

Ivana Bartoletti – Head of Data Protection, Privacy and Ethics

Gemserv

Structure

- **Introduction to data breach notification practices under the GDPR**
- **Data Breach Responses**
  - Key problems and common failures
  - Processes behind the 72 hour breach notification
  - Lessons learnt from cases (Typeform, British Airways, Uber)
- **Notifying Supervisory Authorities**
  - How to communicate effectively with supervisory authorities
  - Third Party notification steps
- **Ongoing Compliance**
  - What are examples of mitigating measures?
  - How to make data protection business as usual
  - Keeping an Incident Log
- **Questions and Answers**
  - Please feel free to pose any questions during the webinar
  - FAQs posed in advance will also be answered



Introduction to Data Breach Notification under the GDPR

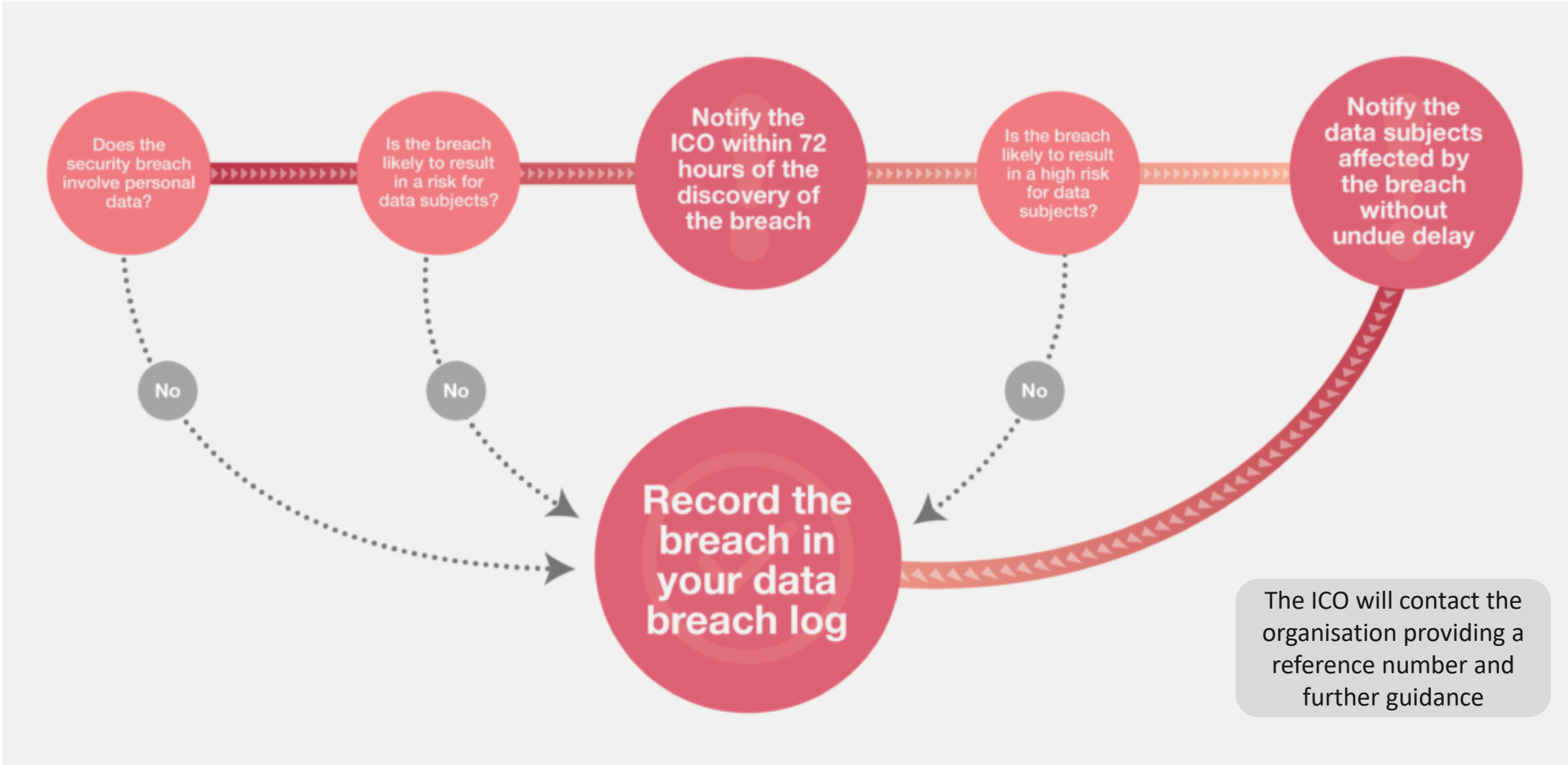
General Requirements

- **Article 33** requires supervisory authorities to be notified of a data breach unless it is **unlikely** to result in a risk to data subjects.
- **Article 34** requires data subjects themselves to be notified if the data breach is **likely** to result in a **high risk** to them.

Other factors

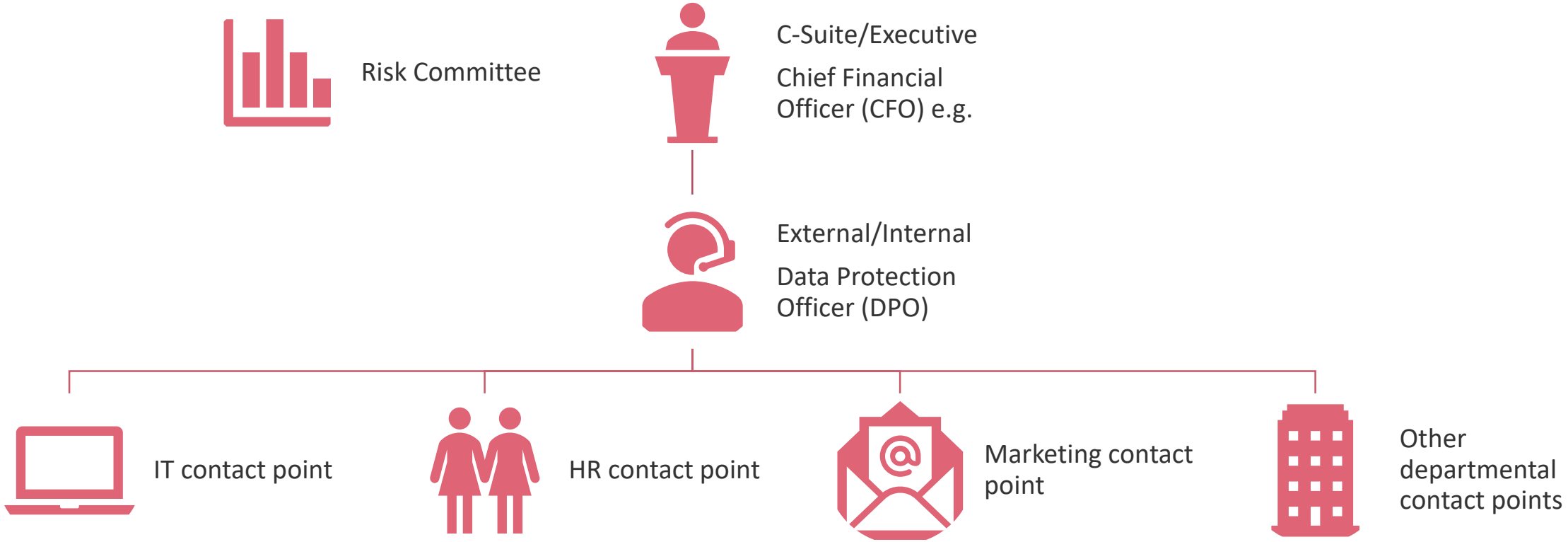
- **Organisations** should notify the supervisory authority in member state(s) where it has an establishment and/or where data subjects will be affected.
- **Notification may not be required** where the organisation has implemented appropriate security measures to contain the breach.

Processes behind the 72-hour breach notification



The ICO will contact the organisation providing a reference number and further guidance

Breach Reporting Structure



Key Factors in determining the impact of a data breach

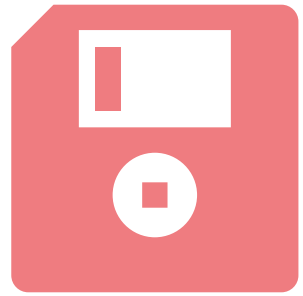
The following factors should be considered:

- Has encryption been used for the data storage?
- Did the data contain special category personal data?
- Does the data contain financial information likely to be used for identity theft?
- How many individuals were affected?

An encrypted hard-drive is stolen that contains the personnel files of employees at an large fashion retailers. This data is also backed up in cloud storage. As it is unlikely that the thieves will be able to access the data, and as it is available elsewhere for employment purposes to the company, notification will most probably not be required.

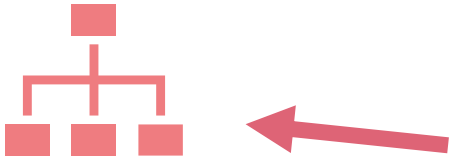
Also consider whether the following have been compromised:

- **Confidentiality**– Preserving restrictions to unauthorised access to and disclosure of personal data.
- **Integrity** - Preventing improper modification or destruction of Personal Data.
- **Availability**– Ensuring timely and reliable access to, and use of, Personal Data.



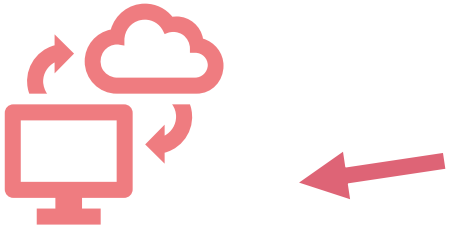
Key Problems and Common Failures

Since the entry into force of the GDPR in May 2018, organisations have faced the following key challenges in complying with data breach notification:



Communication – in particular, involving the need for established procedures and processes and roles and responsibilities for dealing with breaches.

Time windows involve collecting the requisite information on data affected, third party processing and mitigating technical solutions within 3 days.



Responsibility - in particular, involving the need for different organisations or partners to apportion responsibility between them.

Typeform

What are the lessons learned?

- The data breach was remediated within 30 minutes, but it took almost 48 hours for Typeform to investigate the breach and notify it to data controllers.
- Typeform send a comprehensive notice to the customers about the breach and provided a notification template to be used to alert data subjects.

Takeaways for the future:

- **Risk assess a data processor for the security of data processing.**
- **Understand the processor's capacity to report a data breach to you in a timely manner.**
- **Establish deadlines and a form for processors to report a data breach to you.**

Facts:

On 27th June 2018, a Spanish survey company Typeform discovered that an attacker had gained access to their server and downloaded customers' data from an unencrypted back-up.

Customers' payment data and passwords were not affected, but access to email addresses and ID numbers and customers' proofs of residence was gained.

SAs are investigating the matter.

British Airways

What are the lessons learned?

- The data breach was adequately notified to the ICO and affected customers. The details and updates on the situation were also provided to the public.
- British Airways promised to compensate customers who would have suffered from an identity theft or any fraudulent activity.

Takeaways for the future:

- **Decide how is best to escalate a data breach to the public to protect the reputation of your company.**
- **Be prepared to receive SARs and other requests from data subjects.**

Facts:

Customer information from around 380,000 booking transactions made between Aug 21 and Sep 5, 2018, were compromised in a suspected hacking attack.

This included names, addresses, email addresses, and payment card details. Credit card information was put on sale on the dark web.

As of 25th October 2018, criminal and SA investigations are taking place.

Morrisons

What are the lessons learned?

- The Court considered that the organisation's compliance with security obligations under the Data Protection Act 1998 did not preclude its vicarious liability under common law for the employee's criminal actions.

Takeaways for the future:

- **Data breaches can have important reputational and financial implications. News of the leak significantly impacted the value of Morrisons' shares.**
- **Be aware of the threat of rogue employees and detail this as a threat on your risk profile.**
- **Cybersecurity insurance may be the only option to mitigate the effects of unforeseeable incidents.**

Facts:

On 22nd October 2018, Morrisons lost its challenge to a High Court ruling that affected thousands of its employees. This follows a 2014 incident where a former employee leaked such data, including names, addresses, bank account details and salaries, online. Almost 100,000 staff were affected.

The Court found Morrsions liable for breach of confidentiality and misue of private information.

Morrisons has pledged to appeal the case to the Supreme Court.

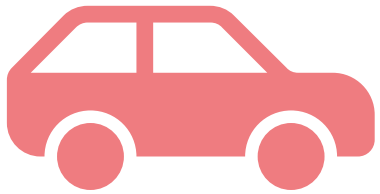
Uber

What are the lessons learned?

- Uber adopted inadequate security arrangements at the time of the data breach.
- Neither SAs, nor data subjects were notified about the breach in a timely manner. This information was escalated by the media with a delay that could severely affect data subjects.

Takeaways for the future:

- **Implement appropriate data security standards and enforce internal policies.**
- **Notify the data breach in time.**
- **In case of a joint-controllership, establish appropriate arrangements in relation to detection, management and notification of data breaches.**



Facts:

In Oct-Nov 2016 attackers gained access to Uber US S3 datastore by retrieving credentials from a compromised Uber repository on GitHub.

32 million non-US Uber users' and 3.7 million drivers' data was illegally accessed.

The attackers demanded a payment from Uber for the disclosure of vulnerabilities. The payment was granted under the "Bug Bounty" programme.

Last week, administrative fines were issued by the UK and Dutch SAs amounting to almost 1 million euros.

Notifying Supervisory Authorities

Tips on notification to supervisory authorities

We suggest the following:

Communication – Answer any specific questions that Supervisory Authorities have and be prepared to meet any deadlines or information/policy/document requirements that they have. Follow the appropriate and particular procedures that the supervisory authority has.

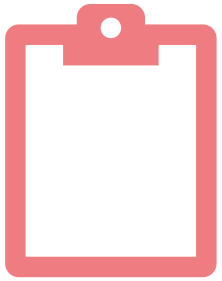
Provide an objective assessment of any incidents that occurred and your interpretation of the requirements, as applied in the business. Additionally, if you are waiting for information, e.g. from your IT suppliers, make this clear.

Describe any mitigating measures you have introduced, including technical measures, where relevant. However, do not feel the need to go into detail on any activities or operations that you carry out where these will not help the enquiry or investigation.

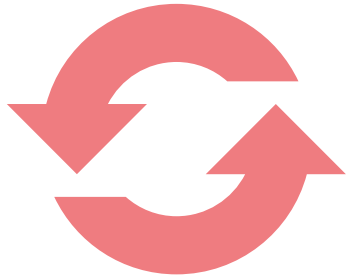
Third Party Notification

Organisations should consider the following steps:

- Agree clauses with relevant third parties.
- The content of these will differ depending on data controller-processor/joint data controller relations.



- Document the breach notification procedure required.
- Evidence the measures yourself and such parties take in relation to each incident.



- Where your organisation is a data processor, you may also have notification obligations to meet.

Ongoing Compliance

What are the relevant mitigating measures?

We suggest the following:

Lock-down access to the origin of the breach or contain any systems to which unauthorized access is possible or may be rendered possible. You may also want to contact searches to see if lost devices can be found, if relevant.

Ensure that services can be continued to be provided to customers and employees despite the data breach/incident. This can include Business Continuity measures.

Educate appropriate staff and contractors. This could involve issuing new guidance.

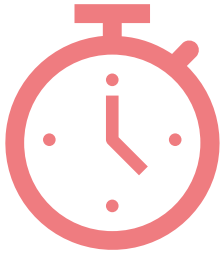
Inform individuals, including possibly data subjects, who can take self-help action. Where relevant, the police should also be informed.

Ensuring business as usual

Organisations should consider the following steps:

- Monitor the impact to the business and individuals
- It may be worth conducting a Data Protection Impact Assessment or Risk Assessment on a breach occurring again

- As part of accountability:
  - record the incident and actions taken in the Incident Log.
  - Discuss ‘lessons learned’ and how to take forward required actions.



- Ensure all policy processes/procedures for notification are made available.
- Carry out regular employee training and monitoring.
- Carry out a table-top exercise or testing scenario.

Keeping a Incident/Data Breach Log

No.	Incident Description	No. subjects affected	Mitigating Action Required	Remedial Action Required	Notification to data subject	Notification to SA
1	Theft of laptop containing staff records				☐	☐
2	Cyberattack affecting online forms used for client surveys				☐	☐
3	Burglary resulting in loss of laptops and financial records				☐	☐
4	Unauthorised access to database of patient records				☐	☐

An Incident Log, whilst not a legal requirement, can aid with compliance.

Questions and FAQs

Please feel free to submit your questions and queries

Q&A

Should companies inform data subjects of a data breach as a matter of course? What constitutes high risk?

What is considered ‘high risk’ should involve considering:

- Ease of identification of individuals - if the individual is unlikely to be directly identifiable by the data (i.e. only pseudonymous data such as CookieIDs are involved), you might not to notify.
- Severity of consequences for individuals - Consider what the impact to them financially or to their reputation may be. Consider whether there is a possibility for identity theft – does the data involve financial info or payment details. Consider whether the data is already publicly available – e.g. where, for example, business contact details are leaked that are available on clients’ websites, this might not be notifiable.
- Special characteristics of the individual - special category personal data (e.g. health data), large amounts of personal data.
- This should be assessed on a case-by-case basis.

Q&A

When a potential breach is discovered should it be considered a data incident that should be investigated before it is concluded it is a breach?

In general yes, since it is not every time it is possible to say that any personal data was affected. If the incident proves that ***personal data was affected***, it must be treated as a **data breach**. Also, remember that, as discussed, not every data breach is notifiable.

Can you think of a good way to ensure processors are following the controllers terms?

You should think about the most important terms to be agreed with processors – which will typically be around data breach notification, following your instructions, and data security. You can conduct a due diligence exercise, asking them for the relevant policies and procedures that they have in place to demonstrate their records and compliance. You can also include a **right of audit** in this – including, for example, for you to audit their data security.

Q&A

At the time of reporting the breach to the SA - what depth of and certainty of information is required?

You can provide a briefer notification within the 72-hour window, and outline to the SA that you will provide more information at a later stage. This might be applicable if you are waiting for an update into a security investigation by your third-party IT provider, for example. Also, you can provide more information at a later stage if there is a relevant update – such as if a stolen laptop is found.

In a situation where there are joint controllers- are both parties required to report?

It depends on the type of an agreement. When it is a **joint-controllership agreement**, parties must agree who and when notifies a breach - in general only **one of them do that**. This should be agreed in contracts with them. When there is an agreement between **separate controllers**, the one whose data subjects are affected or both of them will have to notify.

Does the 72 hours requirement start from when the processor realises the breach or when the controller is notified?

From when the controller is notified.

Q&A

How far should small businesses go in order to protect data? There is a lot of cost associated with putting in the documentation, procedures for dealing with data subject rights and then updating security and company practices to secure the data. Where do you draw the line? I know its all about mitigating against risk but sometimes that is harder said than done.

The GDPR requires to use a **risk-based approach,** meaning that the measures and safeguards to be put into place should be chosen considering a variety of factors. These should include:

- types of personal data processed (the more sensitive types of personal data, such as health or financial, will require higher security and other protective measures)
- categories of data subjects (children's data will require more protective measures, for example)
- data retention periods
- parties with whom the data is being shared (some third-party processors may have a higher risk than others, e.g. those outside the EU).

Organisations must put in place achievable measures. The first step to decide which measures to take is to conduct a data mapping exercise, understand business needs for the data processing, and what can be done to employ good safeguards. Everything must be taken into consideration, and this will help demonstrate accountability to supervisory authorities.

Q&A

If a customer tells you not to contact them but their data was involved in a breach where would you stand on being able to inform them of the breach?

If you determine that a data breach poses a high risk to a particular data subject, you **can** legally contact them solely for the purpose of the notification. However, if a customer has told you not to contact them, it is questionable why you will still keep their contact details on file in the first place. You can also post a **public notification** of the data breach on your website, although this is less preferable to direct data subject notification and should only be used where it is too difficult or expensive to notify each individually.

Can you please explain how to mitigate measures when you play the role of both data controller and data processor?

The mitigation should be done for both of them separately, since the requirements under GDPR are different. You will typically be a data controller for separate data to where you are a processor – you cannot be the same for both.

Q&A

When you log the incidents would it not be a good idea to log the date of incident, date of reporting to ICO, date of further action etc to see how long it takes on each case? Case 1 - 4 days to investigate, 2 days to report to ICO, total time taken. This would allow a business to see the time spent handling data breaches.

Yes, you can implement it this way. This is not required by the ICO or other supervisory authorities, and they will generally take the time of your email to them (sent with the notification form) as the time you notified.

What breach prevention mechanisms would be considered adequate / sufficient with respect to the Morrisons case? What is most critical to focus on?

Create a risk profile of rogue employees. This should include revoking their access controls, or even of not allowing access to employees during disciplinary procedures. Also, if you have taken all the data security measures possible, consider cyber insurance.

Thank you for listening

Please feel free to contact us to find out more about our services:

dataprotection@gemserv.com

Virtual Data Protection Officer | Outsourced Data Protection Officer | EU Representative | Digital Transformation | AI and Data Ethics | ISO 27001 | PCI DSS

Gemserv

INVESTORS IN PEOPLE | Gold Until 2020

bsi. ISO/IEC 27001 Information Security Management

GlobalGROUP ISO 14001 UKAS MANAGEMENT SYSTEMS 0039

LLOYD'S REGISTER LRQA ISO 9001 UKAS MANAGEMENT SYSTEMS 001

CYBER ESSENTIALS PLUS