Colleague Guidance – Dealing with Data Breaches

1) What is a personal data breach?

The law defines a personal data breach as *"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed"*.

What does it mean in practice? It means that someone's personal data has been lost, destroyed, stolen, modified in any way without their consent, disclosed to or shared with other people unlawfully, or it has become unavailable.

Examples

- A member's personal data is accessed on our systems by an unauthorised third-party contractor;
- Customers' personal data is deliberately or accidentally deleted, or not processed as it should have been, by a colleague in Funeral or one of their third-party service providers;
- A colleague in PSG has sent a colleague's personal data to an incorrect recipient;
- Colleagues' laptops and mobile phones are left in cars overnight and get stolen;
- A member's personal details are changed by a colleague in Membership without the member's permission or knowledge;
- Our IT systems have been hacked or encrypted criminally (eg. ransomware), or there is a system outage, or any other type of incident that affects servers and devices, eg. a fire, and personal data becomes inaccessible.

2) What does the law say about data breaches?

The **GDPR (General Data Protection Regulation 2016)** crops up quite a bit in conversations since its implementation in 2018. The GDPR introduced a number of obligations for organisations, such as the Society, that process people's personal data, broadly:

- A duty to report certain types of personal data breaches to the ICO, and notify the **affected individuals** in certain circumstances;
- To ensure that robust breach detection, investigation and internal reporting procedures are in place, and to facilitate decision-making about whether or not a data breach needs to be notified to the ICO and the affected individuals;
- To keep a formal record of any data breach occurring within the Society.

3) What does "affected individual" mean?

When a data breach occurs, not everybody involved in it is automatically an "affected individual". Only the person, or persons, whose personal data has been breached are "affected individuals".

Example

A customer's flight and travelling information is emailed to the wrong customer, by mistake. The email contains their contact details, their itinerary and their bank details as well. The customer who receives the information by mistake contacts our Travel branch, to advise them of the error. The colleague who erroneously sends the email to the wrong customer immediately notifies the Travel's DPCs of the data breach. The DPC notifies the Society's DPM and completes a Data Protection Incident Reporting Form.

Who has been affected by the data breach?

Only the customer whose personal data has been accidentally shared with the wrong person is an "affected individual". The customer who received the information in error, the colleague who caused the data breach, the DPC who notified the data breach and the Society's DPM are not affected parties.

4) So, who does what, within the Society?

The Society's **Data Protection Manager ("DPM")**[1] maintains the formal register of data breach on behalf of Society.

It is also the Society's DPM's responsibility to report data breaches to the ICO, and/or the affected individuals, when necessary.

The Society's **Data Protection Champions ("DPCs")** are the first point of contact for colleagues if they have routine queries about our data protection obligations under the law. There are two designated DPCs in each business group - a contact list can be obtained from the Society's DPM. The Society's DPCs must seek advice from the Society's DPM if unsure about how to proceed when a data breach occurs in their business group, or if they are unable to respond to a colleague's query.

The Society's DPCs are also responsible for completing a **Data Security Incident Reporting Form** when a data breach occurs in their business group. All completed

[1] The GDPR introduced the obligation for certain organisations to formally appoint a Data Protection Officer (DPO). Within the Society, this requirement applies to our Phone Co-op, Healthcare and Energy businesses. The Society's DPM also covers the DPO role.

forms must be sent to the Society's DPM without delay, or in any case as soon as becoming aware of a data breach.

Important → incidents with people's personal data may occur in any business group and at any time, so **it's key that all colleagues know how to recognise a data breach**, and that these incidents are notified to the DPCs, or directly to the Society's DPM, as soon as possible.

Remember, we are all accountable.

5) What if one of our third parties (a contractor, a debt collector, a business partner that processes personal data on our behalf etc.) tells us a data breach has occurred at their end?

All third parties engaged by the Society are bound to contract terms & conditions. If a data breach occurs at their end, they have an obligation to let the Society know about it, and as soon as possible.

If you are told by a third party about a data breach, you must let your DPCs, or the Society's DPM know about it right away. Your DPCs will need to complete a Data Protection Incident Reporting Form and send it to the Society's DPM – they will then assess the best course of action.

6) I am completing a Data Protection Incident Reporting Form, but I don't have all the details yet – what do I do?

Data breaches must be addressed as soon as possible, to limit the consequences these may have on the affected individuals, or the Society.

If you don't know all the facts yet, because your business group is still investigating the incident, **you must complete a preliminary Data Protection Incident Reporting Form**, so that the Society's DPM is aware of the data breach. Remember, data breaches are time critical.

Once more details become known as a result of your business group's investigation, you should complete an **updated Data Protection Incident Reporting Form** and forward it to the Society's DPM.

7) A data breach has occurred, do I need to tell the affected individuals?

The Society's DPM is responsible for notifying a data breach to the affected individuals, if it's deemed necessary under the law. When a data breach occurs, **colleagues must not contact the affected individuals** without having consulted with the Society's DPM first.

It's worth remembering that **not all data breaches need to be notified to the affected individuals** – the Society's DPM will assess each case separately, and it generally depends on the level of risk and the seriousness of the consequences of the data breach on the individuals' freedoms and rights.

8) Do all data breaches need to be notified to the ICO?

No – only data breaches that are **likely to have serious adverse effects** on the "rights and freedoms" of the affected individuals must be reported to the ICO. The Society's DPM will assess each case separately and will follow the necessary course of action. **Not all data breaches must be, or should be, reported to the ICO.**

A number of factors will influence the Society's decision, for example:

a) What's the likelihood and the severity of the risks to the affected individuals?
b) Can the data breach be contained immediately to reduce the level of risk to the affected individuals?
c) What type of data has been breached, and what's the potential impact of the data breach on the affected individuals? For example, loss of control over their personal data, discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality, emotional distress, physical and material damage caused by the data breach.

While data protection legislation only concerns people's rights over their personal data, consideration will also be given, when assessing each data breach, to the level of risk the Society may be exposed, eg. reputational/financial/operational.

If the Society decides the data breach doesn't need to be reported to the ICO, **accurate records of the Society's decision must be made and kept**, for audit purposes, by the Society's DPM.

Example

The theft of a customer database, the data of which may be used to commit identity fraud, would need to be notified to the ICO, given the impact this is likely to have on the affected individuals, who could suffer serious financial losses or other consequences. On the other hand, the Society would not normally need to notify the

ICO, for example, about the loss or inappropriate alteration of an internal Colleague telephone contact list.

If a data breach is reportable to the ICO, the Society's DPM will have to do so "*without undue delay, but not later than 72 hours after becoming aware of the data breach*." The 72 hours deadline starts from when we become aware of the data breach.

Important → Colleagues who become aware or a data breach must contact their DPCs, or the directly the Society's DPM, without delay, so that they can assess the circumstances of the case and decide timely the most appropriate next steps in relation to the data breach.

Failing to notify a data breach to the ICO, when required, is a breach of the law, and the Society could suffer significant financial, reputational and operational damage as a result of such failure.

9) Do all data breaches need to be notified to the affected individuals?

No – only data breaches that are **likely to have serious adverse consequences** for the affected individuals' rights and freedoms must be notified to them.

Again, the Society's DPM will need to assess both the severity of the potential or actual impact on the affected individuals as a result of the data breach, and the likelihood of this occurring – if the impact of the data breach is severe, the risk to the affected individuals is higher. Equally, if the likelihood of the adverse consequences occurring is greater, then the risk to the affected individuals is higher.

The Society will assess each data breach separately and choose the adequate course of action. If a data breach needs to be notified to the affected individuals, the Society will need to do so as soon as possible, particularly if there is a need to mitigate any immediate risks to the affected individuals. One of the main reasons for informing the affected individuals timely is to help them take steps to protect themselves from the effects of a data breach, eg. change their log in details or contact their bank.

Examples

A hospital suffers a data breach that results in the accidental disclosure of patients' records. There is likely to be a significant impact on the affected individuals because of the sensitivity of the data and their confidential medical details becoming known to others. This is likely to result in a high risk to their rights and freedoms, so they would need to be informed about the data breach as soon as possible.

A university experiences a data breach when a member of staff accidentally deletes a record of alumni contact details. The details are later re-created from a backup. This is unlikely to result in a high risk to the rights and freedoms of those individuals; therefore, they don't need to be informed about the data breach.

Healthcare suffers a data breach that results in an accidental disclosure of customers' health records, or a customer is dispatched someone else's prescription in error. There is likely to be a significant impact on the affected individuals because of the sensitivity of the data and their confidential medical details becoming known to others, or even the risk of death if a patient takes the wrong medication in error. Given the margin of risk, similar incidents would need to be notified to the affected people without delay.

10) Is there anyone else the Society should notify a data breach to?

While it's not a specific legal requirement to do so, depending on the circumstances of each data breach the Society may consider notifying other third parties such as the Police, our insurers, a relevant professional body or bank or credit card company. For example, notifying a bank may help to reduce the risk of financial losses to the affected individuals.

Additionally, some of the Society's businesses are also industry-regulated (eg. Ofsted, Ofcom, IATA, Ofgem, etc.) who may impose reporting obligations. The relevant DPCs will need to discuss any such cases with the Society's DPM directly.

11) Does the GDPR require us to keep a record of data breaches?

Yes - **the Society must keep a record of all data breaches** that occur in any of its business groups. The Society's DPM oversees the correct management of the data breach register.

If you become aware of a data breach (whether in your team or not), you must provide all the available details to your DPCs **without delay**, or directly to the Society's DPM, so that adequate records can be made, and remedial actions taken.

All DPCs have access to a **dedicated data protection drive**. Access is granted, and revoked, by the Society's DPM. There are a number of default folders on the drive, for each of the business groups – DPCs should use the drive to keep records of all data breaches occurred in their business group, for audit trail purposes.

12)Who to contact?

If you have any queries, or are unsure how to proceed, you should contact your business group's DPCs in the first instance. If you don't know who they are, you can obtain a list of contact details from the Society's DPM at: data-protection@midcounties.coop.

Alternatively, the Society's DPM can be contacted by phone: 01926 516 064; and by post: The Midcounties Co-operative, Co-operative House, Secretariat Group, Warwick Technology Park, Warwick CV34 6DA.