(See: Responsible Data for M&E in the African Context)

TIP SHEET 5

Developing a data breach protocol

As you collect, transmit, store, and share increasing amounts of data, the possibility of a data breach increases. A data breach refers to any incident involving unauthorised access to a system containing personal data, theft of a device containing electronic personal data, or loss of physical or electronic data. Data corruption is also considered a data breach, as is any other incident that affects the availability of personal data, such as a ransomware attack. When you hold personal and sensitive data, a breach or leak can expose vulnerable groups involved in your M&E efforts to harm.

Having a *data breach protocol* in place is essential to help organisations prevent data breaches and, if breaches do happen, to respond speedily and appropriately. Irrespective of how well secured data is, the possibility of a breach is always there. For this reason, it is critical to be prepared to react quickly when a breach occurs. A personal data breach is defined 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".

Plan ahead so that you are ready to respond rapidly and appropriately in the case of a breach or leak. Various teams will have a role in preventing and responding to data breaches.

The first step in protecting against a data breach is prevention. Different teams have specific roles in prevention and preparation. The following are important points to consider:

- While all teams might have a role in prevention, a smaller sub-set should be identified as those responsible for managing a data breach, e.g. designated persons from IT, HR, legal, communications/PR, finance, and a member of the team affected by the breach.
- Individuals in the data breach sub-set should receive prior training and meet periodically to discuss their roles and responsibilities so that any breach can be dealt with swiftly and efficiently.
- A simulation exercise should be organised at least once a year to maintain the vigilance of the team in preparation for a possible breach.

ORGANISATIONS AND CONTRACTORS	▪ Ensure that updated data privacy and security protocols are in place in order to reduce the likelihood or severity of potential breaches.
IT	▪ Ensure cybersecurity is top-notch to reduce the possibility of a breach. ▪ Provide guidance on how to manage devices and data security.
HR	▪ Train and orient staff on how to avoid a data breach and how to report a suspected intrusion or breach. ▪ Handle and secure employee data appropriately.
COMMS	▪ Minimise the amount of comms data collected and stored to mitigate potential breach damage. ▪ Follow IT and HR data security policies.
FINANCE	▪ Minimise the amount of financial data collected and stored to mitigate potential breach damage. ▪ Follow IT and HR data security policies. ▪ Engage with Legal to prepare for any financial implications of a breach.
LEGAL	▪ Prepare legal precedent and requirements for handling data and reporting a breach. ▪ Negotiate data privacy requirements and data sharing agreements with partners and contractors. ▪ Determine what the organisation is willing to do in the event of a data breach.
PROGRAMMES	▪ Follow good data privacy and security principles ▪ Minimise the amount of programme and beneficiary data collected and stored to mitigate potential breach damage. ▪ Work with partners to support data privacy and security efforts to help avoid a data breach.

M&E	▪ Use 'privacy by design' principles when designing research or M&E. ▪ Follow sound data privacy and security principles. ▪ Minimise the amount of M&E data collected and stored to mitigate potential breach damage. ▪ Work with partners to support data privacy and security efforts to help avoid a data breach
ALL STAFF	▪ Adhere to IT data security recommendations. ▪ Immediately report any suspected data breaches, including loss of a device or removable drive, potential malware or spyware, or other suspected intrusions into the system.

Reporting a data breach or leak

Many national data privacy laws require that certain types of data breach are reported to a Data Protection Authority. If data was encrypted, or the data was accessed but not misused, or if data was highly aggregated and/or anonymised, potential harm and risk may be minimal, and it may not be necessary to notify any authorities or data subjects of the breach. In most cases, there is a 72-hour time limit for informing Data Protection Authorities of a breach unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. There may also be time frames for directly notifying individuals whose data has been breached. In Nigeria, for example, data subjects must be informed within 48 hours of the Data Protection Commission being notified of any breach of their personal data.

DATA PROCESSORS	▪ Notify the data controller immediately if a breach is suspected.
STAFF	▪ Inform IT immediately if a breach is suspected or a device is lost or compromised.
DATA CONTROLLERS	▪ Inform data protection authorities within 72 hours (Check national laws for specific requirements per country). ▪ Inform affected persons or organisations if there is potential for harm due to the breach.

Responding to a data breach or data leak

1. **Immediately assemble the team responsible for dealing with a data breach.**
   This will likely include a representative from IT, HR, legal, communications/PR, finance, and a member of whichever team was affected by the breach.

2. **Determine what happened and how severe it is.**
   - ☐ What was the nature of the breach or attack?
   - ☐ What was the extent of the breach or attack on the system?
   - ☐ What assets are affected?
   - ☐ What information is affected?
   - ☐ What partners or associates or other networks have been affected?
   - ☐ What are the implications of the attack on the organisation and/or its partners or data subjects?

3. **Immediately work to contain the breach. If a network was affected, disable any connections to the point of the breach to prevent further access.**
   - ☐ Clean the system of any unwanted files that might have been installed and make a detailed report of what has been removed for further analysis at a later point.
   - ☐ Run security patches and software updates.
   - ☐ Isolate critical data, especially any highly sensitive data such as financial data or data of vulnerable or sensitive groups.
   - ☐ Initiate new login procedures to any networks and/or devices.
   - ☐ Uninstall and reinstall affected files and programs.

TIP SHEET 5 (continued)

4. **If the breach was a lost, stolen, or compromised device.**
   - ☐ Determine whether there was any personal or sensitive data about individuals, groups, or partner organisations on the device that could be accessed (based on the types of security and encryption that were on the device).
   - ☐ Determine (if possible) who may have accessed the device and whether they may have an interest in any of the data on it.
   - ☐ Determine whether any harm could come to those whose data was compromised and, if so, what type of harm.
   - ☐ Determine if, based on the applicable laws, it is necessary to report the incident to authorities and/or data subjects.
   - ☐ Determine what response or mitigation efforts will be put in place for partners (clients) and/or data subjects, depending on the type of data that was breached and an assessment of potential harm.
   - ☐ Determine if there is a need for any type of damage compensation or additional support to those who have been severely affected by a data breach and how that would be managed and/or financed.
   - ☐ Determine how to reach and clearly explain the situation to individuals or partners (clients) who may be affected. This should be done in a manner that provides them with the information they need to manage any consequences but should not alarm them or make them anxious or upset.
   - ☐ Prepare and release any necessary public notification or media release about the breach and equip staff with a clear narrative about the breach.
   - ☐ Ensure that contact information is available for anyone who has further questions or requires additional support in relation to the breach.

Roles for different teams in responding to a data breach

The response team generally consists of members from all part of the organisation. Below is a chart that defines what roles would be played by different teams in the event of a breach. If working with other partners or contractors, they will need to be involved and informed as well.

CONTRACTORS AND PARTNERS	▪ Anyone who is processing data on our behalf needs to inform us immediately if a data breach is suspected.
IT	▪ Identify and address compromised data. ▪ Determine the number of records compromised and the types of personal information that they contain. ▪ Support forensic investigation and evidence preservation. ▪ Oversee deletion of malware or hacks and correct vulnerabilities that might have precipitated the breach. ▪ Monitor systems for additional attacks. ▪ Fix gaps in the IT system. ▪ Hire additional expertise that may be needed to identify cause and scope of a breach and the type and location of compromised data.
HR	▪ Keep employees updated about data breaches (depending on how severe). ▪ Decide on appropriate action if the breach is linked to a particular employee or their actions.
COMMS	▪ Draft messaging to inform different stakeholders of a breach (where necessary) and mitigate any brand or reputational damage. ▪ Respond to any media inquiries. ▪ Provide reassurance that the breach is being handled.
FINANCE	▪ Determine the financial impact of a breach and recommend budget parameters to respond to the breach. ▪ Work with any vendors affected by the breach.

TIP SHEET 5 (continued)

LEGAL	▪ Advise on response notifications to affected individuals, media, law enforcement, internal teams, government agencies, financial institutions or other third parties. ▪ Review contractual requirements in the case of a breach involving a partner or third party. ▪ Prepare for any post-breach litigation. ▪ Notify regulators and law enforcement. ▪ Alert credit card/credit reporting agencies if needed. ▪ Review contracts to understand any obligations. ▪ Help manage breach investigations and evidence preservation. ▪ Review communications for potential liability.
PROGRAMMES	▪ Work with partners in the event of a data breach.
M&E	▪ Work with partners in the event of a data breach.
ALL STAFF	▪ Keep contacts and partners informed as directed by the incident response team.

☑ Recovering from the initial data breach crisis and lessons to be learnt to improve responses to future crises

- ☐ Appoint a specific person to handle future questions or communication about the breach.
- ☐ Prepare a final report for the files as well as for local authorities or clients on the response effort.
- ☐ Use the data breach experience to improve response systems and ensure that learning is applied in the event of a future data breach.
- ☐ Continue to educate and make staff aware of data privacy and security protocols to prevent future breaches.