

PROCEDURE ON REPORTING PERSONAL DATA BREACHES TO DATA SUBJECTS

SUMMARY

This procedure is about how to notify an individual about a data breach affecting their personal information. The main points are:

- We are required to tell individuals about a personal data breach that may cause them damage, affect their rights, or go against their interests.
- Data breach notifications need to be published very quickly and must be accurate.
- The [Personal Data Protection \(“PDP”\) Team](#) makes a recommendation to Legal on the requirement to notify and helps to draft the notification.
- The final language in the notification must be approved by Legal.

Important to remember:

1. A breach can be intentional or accidental. A breach is any unauthorized disclosure, leak, alteration, access, loss, or destruction of data.
2. Immediately report a personal data breach to [Cyberincidents@kaust.edu.sa](mailto: Cyberincidents@kaust.edu.sa) and DPO@kaust.edu.sa.

FREQUENTLY ASKED QUESTIONS

1. When must KAUST notify individuals about a personal data breach?

KAUST must notify individuals **without undue delay** if a breach may cause damage to their personal data or conflict with their rights or interests.

2. Who decides whether notification to impacted individuals is required?

The PDP Team recommends whether notification is necessary, and Legal makes the final decision.

3. Who is involved in drafting the notification?

The PDP team will support drafting in coordination with the unit stakeholders, Information Security stakeholders, Legal, and GBC.

4. Who approves the final notification before it is sent?

Legal must approve the final wording in a notification.

5. What does the unit need to do after the notification is sent?

Provide a copy of the notification to DPO@kaust.edu.sa and store the breach notification records for 5 years.

6. Who handles follow-up questions from impacted individuals?

Follow-up communications are managed by the PDP team and Legal.