In the event of a data breach for the Oceania Tennis Federation the following steps will be taken:

1. Assess the Threshold

- Evaluate whether the incident risks physical harm, financial fraud, identity theft, psychological distress, or employment damage.
- **Use the Self-Assessment Tool:** Run the situation through the Office of the Privacy Commissioner | NotifyUs portal to decide if it crosses the legal threshold for a notifiable breach.

2. Notify the Privacy Commissioner

- Report to the Privacy Commissioner within 48 hours of becoming aware that a notifiable breach has occurred.
- File the report online using the Office of the Privacy Commissioner | NotifyUs of a serious privacy breach form.
- Provide organisation contact info, the breach timeline, the number of people affected, the types of personal data exposed, the root cause, harm assessments, and mitigation steps taken.

3. Notify the Affected Individuals

- Contact the affected members, coaches, officials, players, or parents directly via phone, email, letter, or in person as soon as practicable with details of what happened and what personal information was involved. Steps the OTF has taken to contain or respond to the breach. Practical steps the individuals can take to protect themselves (e.g., changing passwords, monitoring bank accounts) whilst Confirming that the Office of the Privacy Commissioner has been notified.
- If direct contact is impossible, too expensive, or would cause further harm, each relevant/applicable member federation will be notified directly so as to inform the affected individual.

4. Notify World Tennis

- Contact World Tennis if the affected breach relates to any of their data platforms. Outline the steps the OTF has taken to contain or respond to the breach.

5. Notify the OTF Board

- Prepare a summary report for the Board outlining the steps the OTF has taken to contain or respond to the breach. This report should also assess the cause and provide the practical steps that have been taken to fix the cause and to mitigate the risk of a similar breach occurring in the future.