Protocol for Personal Data Breaches

1. Introduction: our responsibility

As a study association at Radboud University, Maizena handles the personal data of many individuals, including our members, other event attendees, and speakers. The General Data Protection Regulation (GDPR), known in the Netherlands as the Algemene Verordening Gegevensbescherming (AVG), requires us to protect this data and have a clear plan for when things go wrong.

This document is Maizena's official protocol for responding to a personal data breach, designed to ensure we act in full compliance with our legal obligations under the GDPR. A data breach is any security incident that results in the accidental or unlawful loss, alteration, or unauthorized disclosure of personal data.

Our primary goal is to respond quickly and effectively to protect the personal data of every individual we interact with and to comply with the law. We are not alone in this; Radboud University has expert teams to help us, including the FG-Bureau (Data Protection Officer) and CERT-RU (IT Security). This protocol ensures we work with them correctly.

2. What is a personal data breach?

The GDPR, in Article 4(12), 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...". This includes incidents such as:

- *Accidental disclosure*: Sending an email with a list of event participants' names and dietary restrictions (which can be considered sensitive health data under GDPR Article 9) to the wrong person or using 'CC' instead of 'BCC' for a mass email.
- *Loss of device*: A board member losing a laptop or USB stick that contains a file with personal data (e.g., registration lists, contact details).
- *Unauthorized access*: A former board member still having access to Maizena's Google Drive and viewing current member data.
- *Cyber incident*: A phishing attack that gives an unauthorized person access to a board member's account containing personal information.
- *Data unavailability*: Accidentally deleting the only copy of the registration list for an upcoming symposium.

3. The data breach Process in three phases

When a data breach occurs, response is structured in three distinct phases: Immediate response, Management & resolution, and Follow-up & prevention.

Phase 1: Immediate response (the first 24 hours)

This phase is about speed and containment. The goal is to stop the breach and activate the official reporting channel.

1. Discover & contain: The person who discovers the breach takes immediate steps to stop further data exposure and instantly alerts the Maizena board member.
2. Internal alert: The board member informs the entire board that a potential incident is underway.
3. Report to Radboud University (CRITICAL): The board contacts CERT-RU to formally report the incident, in line with GDPR Article 33. This step is mandatory and time-sensitive.

Phase 2: Management & resolution (The next 72 hours)

With guidance from the university, we now work to understand and manage the situation.

4. Investigate the incident: The board, supported by CERT-RU and the FG-Bureau, investigates to determine what happened, what data was affected, and who is impacted.
5. Assess the risk: The board works with the FG-Bureau to evaluate if the breach is "likely to result in a high risk to the rights and freedoms of natural persons," the threshold for notifying individuals under GDPR Article 34.
6. Notify affected individuals: If a high risk is confirmed, the Board, following the FG-Bureau's advice, will send a clear and transparent notification to the affected people explaining the situation.

Phase 3: Follow-up & prevention (after the incident)

Once the immediate crisis is over, we focus on long-term solutions.

7. Implement corrective measures: The board fixes the root cause of the breach and implements new procedures or technical controls to prevent it from happening again.
8. Document everything: The entire incident, from discovery to the final solution, is documented in Maizena's internal Breach Register for legal compliance and future reference, as required by GDPR Article 33(5).

Step-by-Step Procedure

4. The immediate response plan: what to do immediately

If you discover a potential data breach, time is critical. Follow these steps immediately.

Step 1: Stop the breach & inform the board chair

- If possible, take immediate action to limit the damage (e.g., recall the wrongly sent email, take a public Google Form offline, change a compromised password).
- Immediately inform Maizena's board chair. Provide all the details you have. The board chair is responsible for informing the rest of the board.

Step 2: Contact Radboud University (THE MOST IMPORTANT STEP)

Under GDPR Article 33, a data breach must be reported to the Dutch Data Protection Authority (Autoriteit Persoonsgegevens) within 72 hours of becoming aware of it. Radboud

University handles this official reporting, so they must be informed as soon as possible to give them enough time to report the breach.

- The board must contact CERT-RU (Computer Emergency Response Team) at cert@ru.nl. Find more details at https://www.ru.nl/over-ons/beleid-en-regelingen/privacy-en-informatieveiligheid/kwetsbaarheid-melden

Step 3: Action

Call the ICT Helpdesk (icthelpdesk@ru.nl) and seek any help required to handle the potential data breach.

- During office hours: 024-362 22 22 or Erasmuslaan 36, 6525 GG Nijmegen

Do not delay this step. It is better to report a potential issue that turns out to be minor than to report it too late. CERT-RU will guide you on the next steps.

5. Follow-up procedure

Step 4: Investigation (with Radboud's help)

The Maizena board will gather information to answer these key questions:

- What happened? A detailed description of the incident.
- What data was involved? Was it basic contact info, or special categories of personal data (as defined in GDPR Article 9), such as health data (allergies), political opinions, or racial/ethnic origin?
- Who is affected? How many individuals are involved (members, non-members, etc.)?
- What are the potential consequences? Could this lead to identity theft, financial loss, or discrimination for the people affected?

Step 5: Notifying affected individuals (data subjects)

As required by GDPR Article 34, we must notify the affected individuals without undue delay if the breach is "likely to result in a high risk to their rights and freedoms." The FG-Bureau will provide the final assessment on this.

Notification is **not** required under the following conditions, as outlined in Article 34(3):

> (a) The data was protected by measures that make it unintelligible (e.g., strong encryption).
>
> (b) We took subsequent measures that ensure the high risk is no longer likely to materialize.
>
> (c) It would involve disproportionate effort. In this case, a public communication (e.g., a notice on our website) must be made instead.

Step 6: Documentation

GDPR Article 33(5) requires Maizena to maintain an internal record of every data breach, regardless of whether it was reported to the authorities. The board will maintain a "Breach

Register" that documents the facts of the incident, its effects, and the corrective actions taken. This log will be securely stored.