NEWS RELEASE **10 May 2024**

Be prepared: what you can learn from local data breaches

The Office of the Data Protection Authority (ODPA) has released the latest statistics of personal data breaches reported by local organisations, together with what can be learned from them. This information is aimed at all organisations looking to improve their breach preparedness.

A total of **42** personal data breaches were reported to the ODPA during Q1 2024. This is the highest number ever reported in one quarter, with **1,536** people affected.

The following key points can be learned from these most recent breach incidents:

1. **Wayward emails**
   Observation: The long-established trend of emails containing personal data being sent to the wrong person continues to be the most common reported breach. In Q1 2024, **23 of the 42** incidents reported happened due to this reason.
   Learning: Organisations can take steps they to reduce this risk - more information can be found in the ODPA's webinar 'Data breaches human error vs technology' and podcast 'Data breaches: 10 pitfalls & why caring for our data matters'.
   See Figure 1 for a breakdown of all factors that led to the breaches reported in Q1.

2. **Risk assessment**
   Observation: If you work with people's data it is essential you understand how to accurately assess the risk someone may be exposed to if their information is affected by a breach. In Q1, **998** people's data were affected by incidents that the ODPA assessed as being high risk.
   Learning: If you become aware of a data breach you must assess whether there is a risk to the significant interests of the people whose data is affected. In addition to the sensitivity of the information breached and the number of individuals affected, consider the nature, scope, context and purpose of the processing. Remember that sensitivity can be context-specific. A wayward email identifying tennis club members would clearly be less sensitive than one identifying individuals participating in a cancer treatment program. And a breach of even one individual's personal information can be high risk given its sensitivity and the potential for financial, reputational or psychological harms.
   See Figure 2 for more details on the assessment of risks posed by the breaches reported in Q1.

3. **Potential harms**
   Observation: To help you assess the risk posed by a breach it is important to understand the types of harm they may cause. In Q1, **23** of the breaches reported pointed to 'loss of confidentiality' as a potential harm whilst **13** breaches pointed to 'emotional distress'.
   Learning: 'Data harms' are real and often cannot be undone, so organisations can mitigate the risk

of them occurring by developing a deeper understanding of harms. A part of this is recognising that you may not have the full picture of how vulnerable a person may be if their information is compromised, as it is entirely context-driven.

See Figure 3 for a full breakdown of the potential harms identified by organisations reporting breaches during Q1.

4. **Rely on your people and heed system warning signs**

   Observation: The vast majority of breaches reported during Q1 were discovered by people, just **2 incidents out of the 42** reported were detected through system auditing or testing. Learning: It is important to nurture a culture where the people in your organisation are encouraged to internally report any breaches they discover. Relying on your people in this way gives you the best possible chance of acting quickly to contain a breach and mitigate its effects. When it comes to audits and system monitoring, when these tech tools do detect anomalies, heed those warning signs and investigate. Many breaches can be avoided by ensuring follow-up on systemic red-flags.

   See Figure 4 for a full breakdown of how organisations discovered breaches during Q1.

5. **Know whose data you have**

   Observation: People are at the heart of each breach reported. Of the breaches reported in Q1, incidents involved: child patients, adult patients, vulnerable patients, staff/volunteers, students, service users, and customers.

   Learning: It is important to consider the nature of your relationship with the people affected to inform your risk assessment.

   See Figure 5 for a full breakdown of the relationship between the human beings affected by the breaches reported by organisations during Q1.

6. **How personal is the personal data**

   Observation: In Q1, **15 breaches involved 'special category data'**, specifically, information relating to people's health, biometrics, trade union membership, and alleged criminal activity.

   Learning: Different types of information about a person carry different levels of risk. This is why local data protection law distinguishes between 'personal data' and 'special category data'. Special category data is anything that reveals an individual's racial or ethnic origin, political opinion, religious or philosophical belief, trade union membership, genetic data, biometric data, health data, data concerning an individual's sex life or orientation or criminal data. This type of information is afforded extra protection in the law as it is recognised that this type of data could create more significant risks to a person's fundamental rights and freedoms, for example, by putting those persons at risk of unlawful discrimination.

   See Figure 6 for a full breakdown of the types of personal data affected by the breaches reported by organisations during Q1.

7. **Tell people who may be at risk**
   Observation: In Q1 **13 out of the 42** breaches met the risk criteria where the organisation must tell those people whose data had been affected. However, of these 13 high risk breaches, **only 5** led to the people at risk being told.
   Learning: In almost all circumstances, you are legally obliged to notify people of breaches that you have assessed to be high risk. This allows the people affected to protect to take action to protect themselves from unwanted consequences. However, the ODPA recommends, from an ethical perspective, that you tell people if their data has been involved in any breach, regardless of the risk assessment you make as there may be a specific risk to individuals that you are not necessarily aware of. Furthermore, openness and honesty helps build trust whereas withholding that information could mean someone gets an unwelcome surprise that will adversely impact your relationship with them.

The Bailiwick's Data Protection Commissioner, Brent Homan, commented:

"It is so important to view security safeguards as a dynamic rather than static responsibility. Organisations can think of breach preparedness like cruise control of a car. You can't set it and then jump in the back seat and relax. You must steer carefully, be aware of present dangers to you, your passengers and other road users and be prepared to confront unknown threats awaiting you at the turn of the road. Working with people's data is no different, and we hope that sharing the data-driven insights from the breaches reported locally can help local organisations rapidly and effectively respond when a breach occurs."

You can find more information about how to handle a data breach on the ODPA's website: www.odpa.gg/breach-response. The ODPA are starting a free breach workshop series in the summer – see www.odpa.gg/events for more details.

- ends -

Notes:

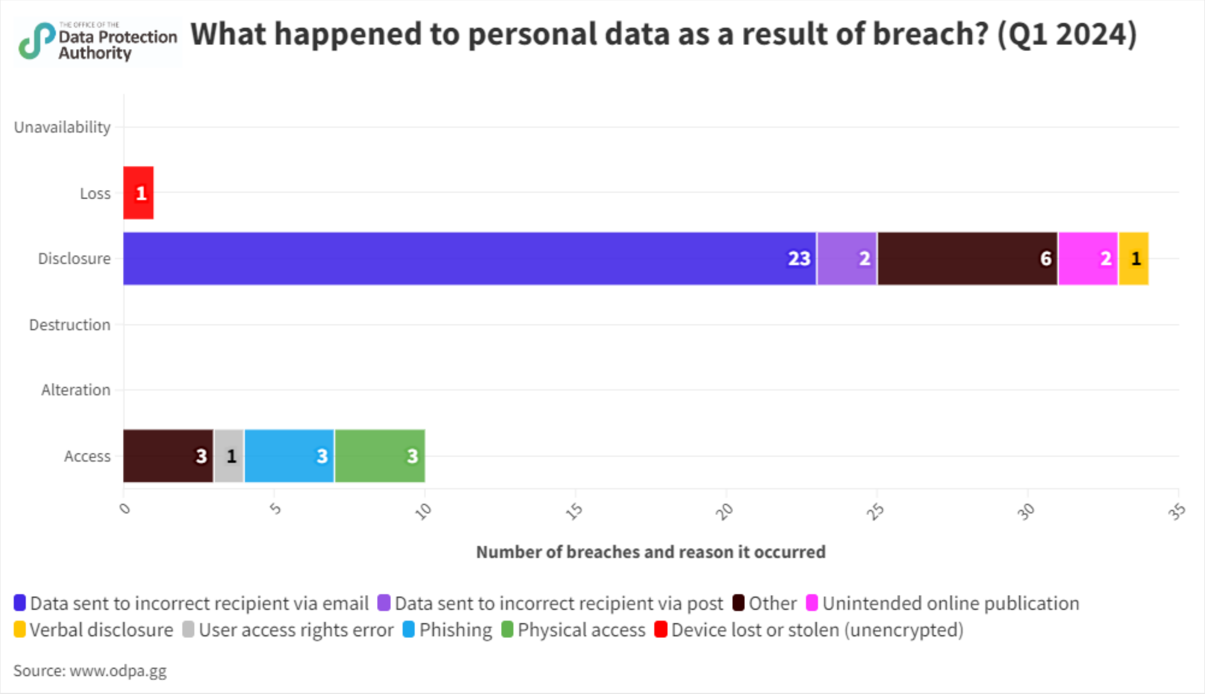
This release is part of the **quarterly breach report statistics** the ODPA has been issuing since June 2018. Statutory breach reporting was one of the key changes to the local data protection law introduced in May 2018. *The Data Protection (Bailiwick of Guernsey) Law, 2017* (section 42) states that organisations are legally required to notify the ODPA of any personal data breach within 72 hours of becoming aware of it.

Breach criteria

A personal data breach is defined in section 111(1) of the Law as any incident that meets the following criteria: "*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*."

There will likely be a breach whenever any personal data is accidentally lost, corrupted or disclosed, or if someone accesses it or passes it on without proper authorisation to do so.

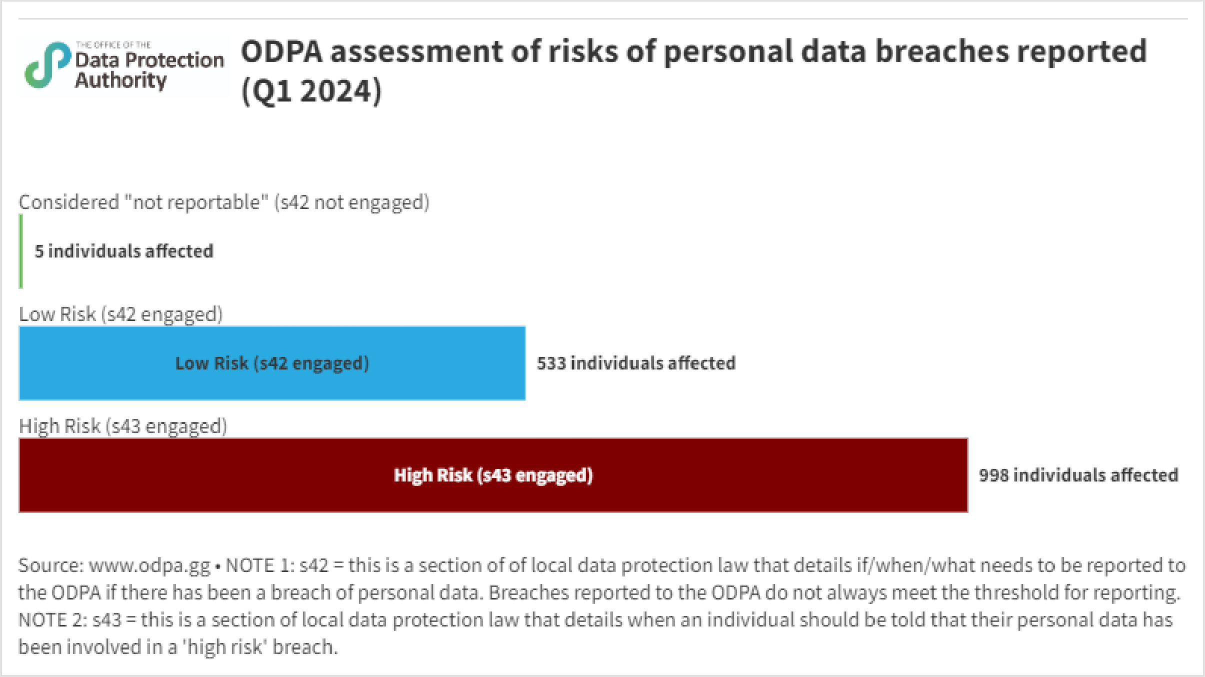
Figure 1



What happened to personal data as a result of breach? (Q1 2024)

Source: www.odpa.gg

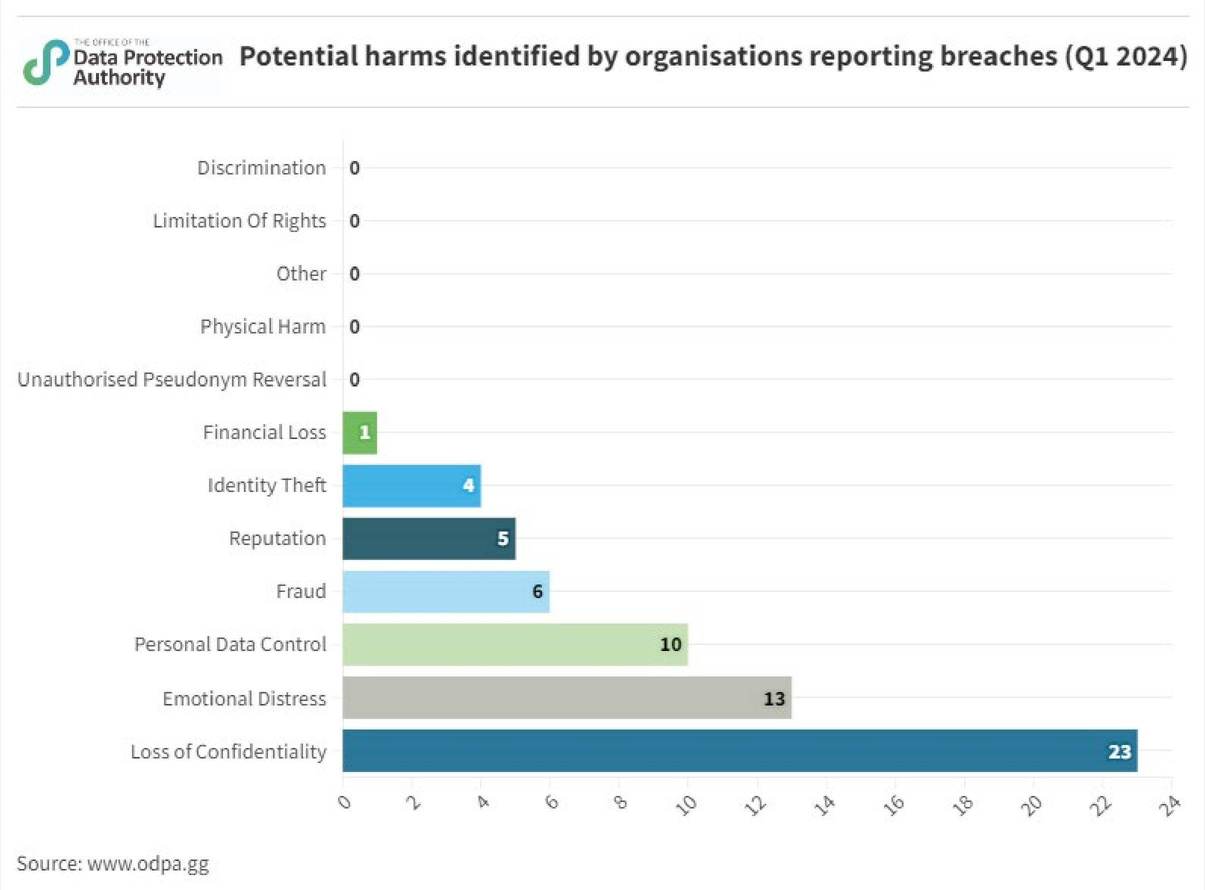
Figure 2



ODPA assessment of risks of personal data breaches reported (Q1 2024)

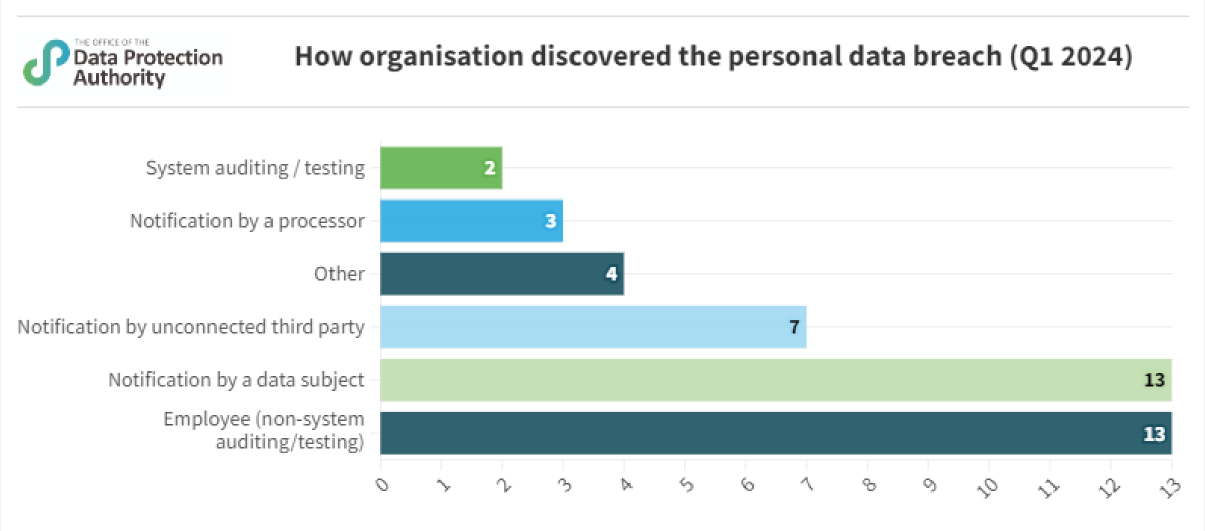
Source: www.odpa.gg • NOTE 1: s42 = this is a section of of local data protection law that details if/when/what needs to be reported to the ODPA if there has been a breach of personal data. Breaches reported to the ODPA do not always meet the threshold for reporting. NOTE 2: s43 = this is a section of local data protection law that details when an individual should be told that their personal data has been involved in a 'high risk' breach.

Figure 3



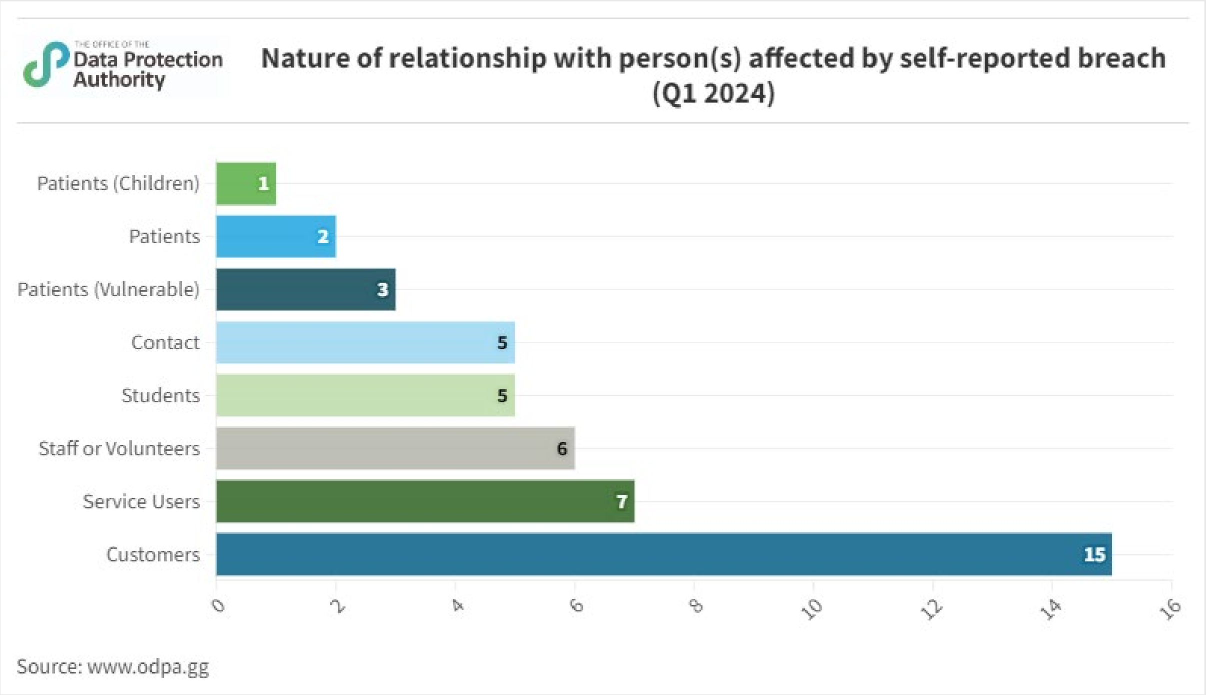
Source: www.odpa.gg

Figure 4



Source: www.odpa.gg • 'Data subject' = the individual whose data was affected by the breach.

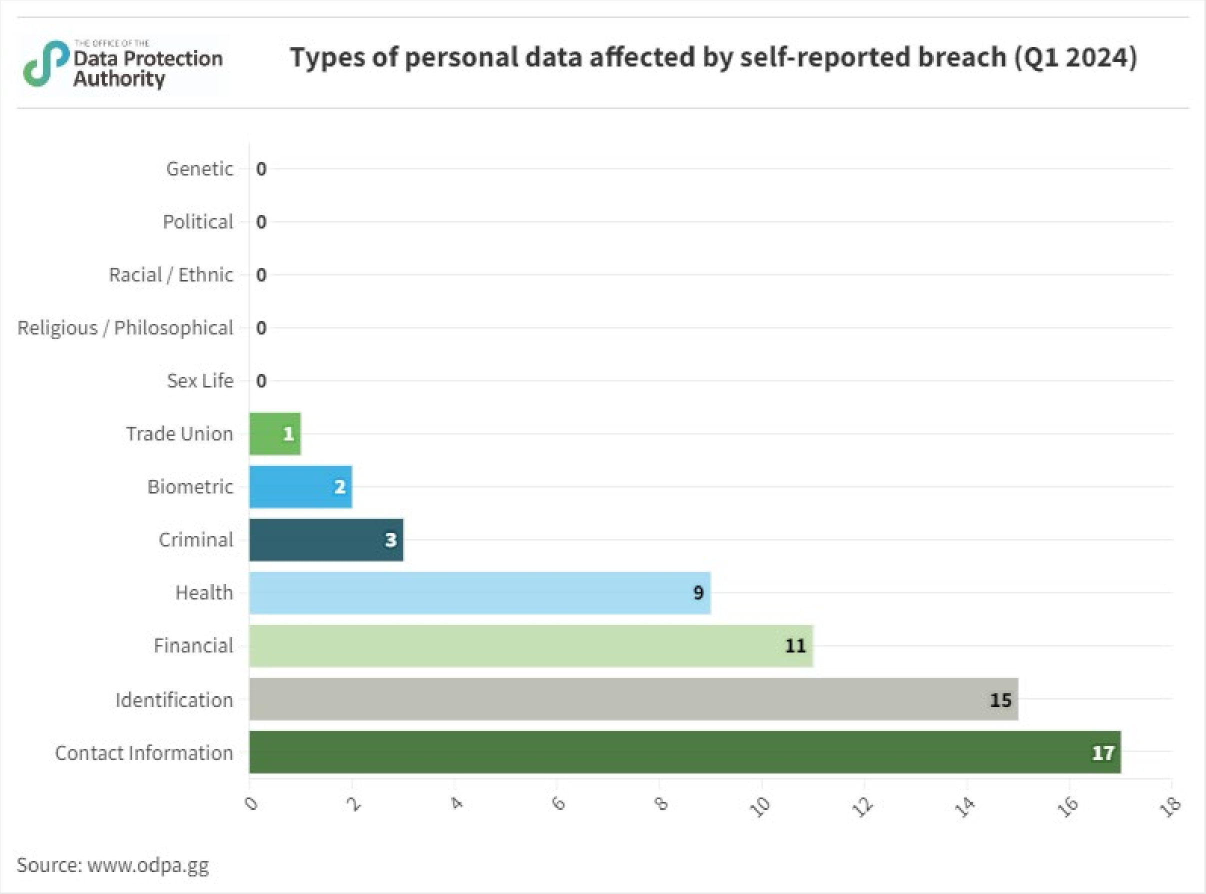
Figure 5



Nature of relationship with person(s) affected by self-reported breach (Q1 2024)

Source: www.odpa.gg

Figure 6



Types of personal data affected by self-reported breach (Q1 2024)

Source: www.odpa.gg