# Over 1 in 3 Businesses at Risk of Being Fined Since GDPR Update, ICO Data Reveals

**Ongoing data published by the Information Commissioner’s Office reveals that 37% of businesses are at risk of huge data breach fines since the GDPR update.**

A recent [study](https://www.hayesconnor.co.uk/news-resources/news/ico-data-security-incident-trends/) from leading UK data breach solicitors, Hayes Connor, has uncovered the industries most affected by data breaches. They analysed the ICO’s ongoing data security report, which shows how businesses have been conforming to GDPR since its inception.

Shockingly, just **1 in 4 data breaches** across all sectors are said to have been **reported in less than 24 hours**. 38% were reported between 24 and 72 hours, whilst **37% were reported after 72 hours**.

Part of the 2018 GDPR regulations require businesses to report a data breach within 72 hours. Failure to notify a breach when required to do so can result in a significant fine of up to £8.7m or 2 per cent of your global turnover. Based on historical ICO stats, over 1 in 3 businesses have been putting themselves at risk of large fines.

The findings have also revealed some other shocking stats, including:

* There have been a total of **32,541 data breaches** reported to the ICO since 2019.
* The **health sector** made up the majority of total data breaches, taking up almost **1 in 5 cases** since 2019.
* The **education and childcare sector** made up **1 in 7 cases**, putting children’s data at huge risk of breach.
* There were approximately **650 cases of children’s data** being breached since 2019.
* **Basic personal identifiers** being breached came up top in over **69% of cases**.
* **80% of data breaches** were **non-cyber related**, suggesting a lack of GDPR training or awareness within businesses.
* The main reason for data breaches across all sectors was data being **emailed to the incorrect recipients**, making up **15% of cases**.

Christine Sabino, Legal Director at Hayes Connor, said, “What’s concerning is the public puts a lot of trust in industries such as the health, government, and education sectors, with the expectation that their data is going to be handled securely.

“With so many of these data breaches being caused by human error, it’s very clear that these industries are in dire need of data handling training, at the very least. With Computer Security Day arising on 30th November, now is the ideal time for businesses to rethink their data handling practices.”

If your personal data has been compromised as a result of security failings by an organisation, you may be entitled to claim GDPR compensation.

Hayes Connor Solicitors have significant expertise supporting clients who’ve had their data exposed due to data protection negligence. They can support claims for privacy loss, distress, and financial losses. Head [here](https://www.hayesconnor.co.uk/contact-us/) to get in contact with them, or make a claim [here](https://www.hayesconnor.co.uk/contact-us/make-a-claim/).

**-ends-**

Hayes Connor is a leading law firm based in Warrington specialising in data breach and protection. For more information on the study, please contact Joanna Cunningham at joanna@conscious.co.uk, Eleanor Dix at eleanor@conscious.co.uk, or Megan Gibbs at megan@conscious.co.uk.

**Data Sources:**

* [Data security incident trends](https://ico.org.uk/action-weve-taken/data-security-incident-trends/) from [Information Commissioner’s Office](https://ico.org.uk/action-weve-taken/data-security-incident-trends/)

**Methodology**

This report has been created with reference to the findings uncovered by the ICO’s ongoing data security report.

The figures provided throughout the report are general averages from 2019-2022 and were taken from the ICO report.

Please keep in mind that, while the data was obtained from reputable sources, the interpretations are that of the Hayes Connor researchers.