| Police Scotland logo | Freedom of Information ResponseOur reference: FOI 25-2289Responded to: 25 August 2025 |
| --- | --- |

Your recent request for information is replicated below, together with our response.

## Please provide the following details for the period from ****1 January 2020 to the most recent available date****:

## ****Number and type**** of cybersecurity incidents recorded, including (but not limited to):

## Hacking incidents

## Phishing incidents

## Malware or ransomware attacks

## Unauthorised access to data or systems

In terms of section 18 of the Act, I am refusing to confirm or deny whether the information sought exists or is held by Police Scotland. Section 18 applies where the following two conditions are met:

* It would be contrary to the public interest to reveal whether the information is held.

Whilst we accept that doing so would better inform the public as to the security arrangements Police Scotland has in place regarding the processing of their personal data, the overwhelming public interest lies in protecting the integrity of Police Scotland systems and processes.

* If the information was held, it would be exempt from disclosure. In this instance, the following exemptions would apply:
* Section 31(1) - National Security and Defence
* Section 35(1)(a)&(b) - Law Enforcement
* Section 34(1)(b) - Investigations

Disclosure would prejudice the prevention and detection of crime and the apprehension and prosecution of offenders.

Furthermore, information is exempt information if it is held for the purposes of an investigation which may result in the submission of a report to the Crown Office and Procurator Fiscal Service (COPFS).

Exemption is further required for the safeguarding of national security.

Whilst we accept that disclosure would better inform the public as to the security arrangements Police Scotland has in place regarding the processing of their personal data, the overwhelming public interest lies in protecting the integrity of Police Scotland systems and processes.

## ****Number of personal data breaches**** reported to the Information Commissioner’s Office (ICO), including breaches relating to GDPR compliance.

## ****Details of breaches****, including:

## Date of each breach

1. August 2020

2. November 2021

3. October 2023

4. August 2024

5. September 2024

6. February 2024

7. October 2024

8. February 2024

9. April 2025

10. June 2025

## Type of data compromised (e.g., names, addresses, medical records, financial details, employment data, etc.)

Name, address, date of birth, contact details, image, fingerprints, health, vehicle registration, data contained on Police databases and applications.

## Number of files or records leaked, compromised, or accessed without authorisation

## ****Number of individuals affected**** by each breach:

## Please break down by staff/public if applicable

Unfortunately, it would cost well in excess of the current FOI cost threshold of £600 to answer these questions. I am therefore refusing to provide the information sought in terms of section 12(1) of the Act - Excessive Cost of Compliance.

To explain, we would need to individually assess each case to identify this information for you. This would cost well in excess of the £600 and 40 hours prescribed by the Scottish Ministers under the Act.

## Whether the affected individuals were staff members, members of the public, or both

Both

## ****Total financial compensation paid out**** to victims of data breaches, including staff and members of the public.

## Please break down the compensation amounts by breach if applicable.

I regret to inform you that I am unable to provide you with the information requested above. Therefore, in accordance with Sections 12(1) (Excessive cost of compliance) and 16(4) (Refusal of request) of the Freedom of Information (Scotland) Act 2002 (the Act), this letter represents a Refusal Notice.

By way of explanation, files which relate to data breaches are not stored under any specific heading.

A data breach file could come under a number of headings, including employers liability claims, public liability claims, legal enquiry, or other.

Police Scotland receive hundreds of possible claims each year and researching this request would require each file to be individually looked at to determine whether it could be classified as a data breach.  This would take on average ten minutes per file and would exceed the £600 and 40 hours prescribed by the Scottish Ministers under the Act.

## ****Brief summary of actions taken by your organisation**** to respond to each breach, including remedial or preventative measures.

Communications to staff providing advice and guidance to prevent future incidents.

Refresher training

Recording/Storage/Department practises reviewed/updated

Audits and compliance

Liaise with Learning and Training department

If you require any further assistance, please contact us quoting the reference above.

You can request a review of this response within the next 40 working days by email or by letter (Information Management - FOI, Police Scotland, Clyde Gateway, 2 French Street, Dalmarnock, G40 4EH). Requests must include the reason for your dissatisfaction.

If you remain dissatisfied following our review response, you can appeal to the Office of the Scottish Information Commissioner (OSIC) within 6 months - [online](https://www.foi.scot/appeal), by email or by letter (OSIC, Kinburn Castle, Doubledykes Road, St Andrews, KY16 9DS).

Following an OSIC appeal, you can appeal to the Court of Session on a point of law only.

This response will be added to our [Disclosure Log](http://www.scotland.police.uk/access-to-information/freedom-of-information/disclosure-log) in seven days' time.

Every effort has been taken to ensure our response is as accessible as possible.
If you require this response to be provided in an alternative format, please let us know.