Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524 510 www.ico.org.uk

[redacted]
Disclosure Officer
Data Management and Disclosure Unit
South Wales Police
Cowbridge Road
Bridgend
CS31 3SU

By email only to: [redacted]

26 August 2022

Dear [redacted]

Case Reference Numbers INV/0770/2020 and INV/0610/2021

I write to inform you that the ICO has now completed its investigation into the disclosure of personal information by South Wales Police on two separate occasions, the first reported was for an incident in April 2020 (the first incident), and a second is an incident that actually predates the first, that occurred in February 2020 (the second incident).

In summary, it is my understanding that for the first incident, reference INV/0770/2020, a woman had her identity disclosed to a partner following her application for information about him under the Domestic Violence Disclosure Scheme (DVDS), also known as Clare's Law. The partner had previous convictions for violence and sexual assault and was being managed by a police officer from South Wales Police who was acting as his Offender Manager. In this incident the identity of the applicant was disclosed during a conversation between the partner and the Offender Manager. [redacted]

In the second incident, reference INV/0610/2021, the data subject involved had her identity disclosed by a police officer after she made an application for information under the Child Sex Offender Disclosure Scheme (CSODS), also known as Sarah's Law. This application was about an offender who was the partner of [redacted]. The identity of the data subject was disclosed [redacted] by a police officer who attended her property in the course of safeguarding duties as a result of the CSDOS application.

This case has been considered under the Data Protection Act 2018 (the DPA 2018) due to the nature of the processing involved.

Our consideration of this case

I have investigated whether South Wales Police has complied with the requirements of the data protection legislation.

In the course of my investigation, I have noted that for the first incident, that the officer involved dealt with the partner as part of their duties under the Multi-Agency Public Protection Arrangements (MAPPA), not under DVDS, and that it was appropriate to be managed under MAPPA in these circumstances.

For the second incident, it was noted that the disclosure occurred under stressful conditions while the police officer was performing their duties in line with safeguarding procedures. At the time the disclosure was made the officer was dealing with [redacted] who was in an extremely emotional and distressed state and that the disclosure was made as part of an attempt by the officer to provide some reason for the police presence at the property.

We have also considered and welcome the remedial steps taken by South Wales Police in light of this incident. In particular, that South Wales Police has taken on board the recommendations made in the report made into the first incident by the Independent Office for Police Conduct (IOPC). It is noted that South Wales Police, in its response outlined some of these measures that have already been taken.

However, after careful consideration and based on the information provided, we have decided to issue South Wales Police with a reprimand in accordance with Schedule 13 (2) of the DPA 2018.

Details of reprimand

The reprimand has been issued in respect of the following processing operations that have infringed Section 40 Part 3 of the DPA 2018:

- Section 40 states that, "data processed for any of the law enforcement purposes must be so processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures (and, in this principle, 'appropriate security' includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage)."

In particular, it was of concern that, officers and civilian staff involved failed to act in a way that would have been expected in order to preserve the identity of the data subjects in both incidents. The consequences of which, had the potential to cause significant damage and distress to each of the data subjects.

It is considered that South Wales Police failed to ensure that its civilian staff and officers had received full and appropriate training to enable them to fully understand the tasks they need to perform in these incidents.

In the first incident, the officer concerned had been in a role as a Management of Sexual or Violent Offenders (MOSOVO) officer [redacted]. However, from evidence provided by South Wales Police, the officer had not received any training in DVDS, and while they had received some training as a Sexual Offences Liaison Officer, they had not completed

the National MOSOVO course, nor had they received any relevant data protection training since July 2018.

For the second incident, the evidence provided showed that the police officer had not received relevant data protection training since December 2018 and had not received training in CDODS since 2015.

Training had not been kept up to date for the police officers and staff involved and South Wales Police did not ensure that training was available, was taken up, and was fully understood by those involved. If this had been done, the officers and civilian staff are likely to have been more mindful when conducting the interactions with the parties involved in both incidents which could have prevented both incidents from occurring.

Furthermore, no appropriate guidance or documented process was in place and available for police officers and civilian staff to understand their roles and responsibilities with regard to what could and what could not be communicated to the parties involved, especially in respect of instances where MAPPA and DVDS overlap. These faults led to personal information being divulged in each of the incidents that resulted in distress to the data subjects concerned.

Consideration has also been given to the fact that South Wales Police was subject to an ICO Audit in September 2019. This audit noted that despite having nationally recognised information governance training, there was no formal training programme in place. It was stated that without an overall training programme there was the risk that South Wales Police staff would not receive relevant and timely information governance training.

The audit report suggested that this may lead to officers and staff not being aware of their responsibilities and increased the risk of a data breach taking place. As such, it is considered that prior to these two incidents occurring, South Wales Police was aware of improvements that were required in respect of training but failed to ensure that appropriate training had been provided to the officers concerned in these two incidents.

Due to this, it is considered appropriate to issue a reprimand for infringements of Section 40 Part 3 of the DPA 2018.

Further Action Recommended

The Commissioner recommends that South Wales Police could take certain steps to improve its compliance with DPA 2018. In particular:

1. That South Wales Police ensure that all recommendations made in the IOPC report are fully and completely implemented. If these have not been done so already, then as soon as is possible.

2. South Wales Police should ensure that lines of communication are clear once an application for information is received so that all police officers and civilian staff are aware of their responsibilities when dealing with disclosures. Furthermore,

officers should ensure that all communications are sent to the correct teams involved.

3. South Wales Police should consider a review of its data protection reporting procedures, and what constitutes as data protection issue, to ensure that all future incidents are reported correctly and within the usual 72-hour timeframe.

Whilst the above measures are suggestions, I would like to point out that if further information relating to this subject comes to light, or if any further incidents or complaints are reported to us, we will revisit this matter and further formal regulatory action may be considered as a result.

Further information about compliance with the data protection legislation which is relevant to this case can be found at the following link:

https://ico.org.uk/for-organisations/guide-to-data-protection/

We actively publicise our regulatory activity and outcomes, as this helps us to achieve our strategic aims in upholding information rights in the public interest. We may publish information about cases reported to us, for example where we think there is an opportunity for other organisations to learn or where the case highlights a risk or novel issue.

Therefore, we may publish the outcome of this investigation to publicise our regulatory authority and new powers under the UK GDPR. We will publish information in accordance with our Communicating Regulatory and Enforcement Activity Policy, which is available online at the following link:

https://ico.org.uk/media/about-the-ico/policiesandprocedures/1890/ico_enforcement_communications_policy.pdf

Please let us know if you have any concerns about this.

Thank you for your co-operation and assistance during the course of our investigation.

We now consider the matter closed.

Yours sincerely

[redacted]
Lead Case Officer
Investigations
Information Commissioner's Office
[redacted]

Please note that we are often asked for copies of the correspondence we exchange with third parties. We are subject to all of the laws we deal with, including the United Kingdom General Data Protection Regulation, the Data Protection Act 2018, and the

Freedom of Information Act 2000. You can read about these on our website (www.ico.org.uk).

The ICO publishes basic details about the complaints, investigations, and self-reported data breaches it handles. These details include the name of the organisation concerned, the dates that we opened and closed the case, and the outcome. Examples of published data sets can be found at this link (https://ico.org.uk/about-the-ico/our-information/complaints-and-concerns-data-sets/).

We do not include personal data in the published datasets and will anonymise the names of sole traders etc prior to publication. We also do not publish cases concerning domestic CCTV complaints and may not publish certain other cases if we feel it is not appropriate to do so in the circumstances.

If you wish to raise an objection to us publishing a case in the datasets, whether or not we have published it yet, please contact us explaining your reasons for this at accessicoinformation@ico.org.uk .

Please say whether you consider any of the information you send us is confidential. You should also say why so that we can take that into consideration. However, please note that we will only withhold information where there is good reason to do so.

For information about what we do with personal data see our privacy notice at www.ico.org.uk/privacy-notice