

# **DATA PROTECTION ACT 2018 AND UK GENERAL DATA PROTECTION REGULATION**

## **REPRIMAND**

The Information Commissioner (the Commissioner) issues a reprimand to Nottinghamshire Police in accordance with Schedule 13(2)(c) of the Data Protection Act 2018 (DPA 2018) in respect of certain infringements of the DPA 2018.

### **The reprimand**

The Commissioner has decided to issue a reprimand to Nottinghamshire Police in respect of the following infringements of the DPA 2018:

- Section 40 Data Protection Act 2018 which states that "The sixth data protection principle is that personal 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)."
- Section 56 of the Data Protection Act 2018 which states that "Each controller must implement appropriate technical and organisational measures to ensure, and to be able to demonstrate, that the processing of personal data complies with the requirements of this Part. (2) Where proportionate in relation to the processing, the measures implemented to comply with the duty under subsection (1) must include appropriate data protection policies. (3)The technical and organisational measures implemented under subsection (1) must be reviewed and updated where necessary."
- Section 57(1) of the Data Protection Act 2018 which states that "Each controller must implement appropriate technical and organisational measures which are designed (a) to implement the data protection principles in an effective manner, and (b) to integrate into the processing itself the safeguards necessary for that purpose."
- Section 66(1) of the Data Protection Act 2018 which states that "Each controller and each processor must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks arising from the processing of personal data."

The reasons for the Commissioner's findings are set out below.

The breach in this case was an unauthorised disclosure of the personal data of witnesses via a police officer's unredacted statement on the CPS Digital Case Management system. The evidence has revealed that in this instance, the cause of the disclosure of the personal data of witnesses was the failure to ensure the adequate redaction of the data before disclosing this to the CPS.

The evidence has further revealed that this failure was due to a lack of proper redaction and/or disclosure training. Therefore it would be reasonably foreseeable that there could be officers completing redaction and disclosure without proper training. [REDACTED]

In addition to this more generally Nottinghamshire Police had no oversight over whether policies regarding redaction and data protection were accessed or understood by officers, instead relying on emails from heads of departments to officers to alert them of any changes in the policy.

Data Protection training was mandatory during induction but there was no oversight over whether this was completed and Nottinghamshire Police are unable to say whether the officers involved in this breach had completed the training. Nottinghamshire Police stated that the completion rate for Data Protection training from 1 December 2020 to 1 December 2022 was 15.85%.

Therefore Nottinghamshire Police failed to ensure appropriate security of the personal data, using appropriate technical or organisational measures in line with Section 40, 56, 57(1) and 66 of DPA18.

#### Mitigating factors

In the course of our investigation we have noted that human error contributed in part to the breach, there was no actual harm caused to the data subjects or any effect on the outcome of the trial.

#### Remedial steps taken by Nottinghamshire Police

The Commissioner has also considered and welcomes the remedial steps taken by Nottinghamshire Police in the light of this incident. In particular Nottinghamshire Police worked with the CPS to remove and retrieve the data and steps were taken to ensure the safety of the data subjects affected. It is also noted that in order to prevent a recurrence of the incident Nottinghamshire Police undertook a review of the department's

policies and procedures and will be implementing a SOP in respect of this process. During this process the Information Management Unit (IMU) identified that additional data protection and disclosure guidance would be beneficial to the whole organisation.

### Decision to issue a reprimand

Taking into account all the circumstances of this case, including the mitigating factors and remedial steps, the Commissioner has decided to issue a reprimand to Nottinghamshire Police in relation to the infringements of sections of the DPA 2018 set out above.

### **Further Action Recommended**

The Commissioner recommends that Nottinghamshire Police should take certain steps to ensure its compliance with DPA 2018. With particular reference to section 40 of the DPA 2018, the following steps are recommended:

1. Consider providing explicit redaction training to employees involved in the disclosure or redaction of evidence.
2. Review data protection training schedules and systems to ensure that adequate monitoring is in place in order to improve levels of compliance and completion.
3. Consider incorporating anonymised examples of incidents into data protection training to raise awareness of the potential for breaches to occur, with particular attention being given to their inclusion in departments where such incidents have occurred.
4. Ensure that the collective learnings from data breaches are shared across the whole force, particularly if the type of processing is common across areas.
5. Complete the implementation of the Standard Operating Procedure, dissemination of guidance and mandatory NCALT Data Protection Training.