Data Protection Breach Policy (Surrey and Sussex) (1180/2025)

Abstract

This document outlines the Surrey Police and Sussex Police duty to report data breaches and the requirement to ensure appropriate steps are in place to contain and mitigate the effects of any data breach.

Policy

1. Introduction

1.1 The UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 (DPA 2018) provides rights to employees and the public about how their personal data is collected, processed, stored, and shared. The purpose of this policy and procedure is to ensure that all Surrey Police and Sussex Police (hereafter referred to as the Forces) officers, Special Constables, staff, and agents (hereafter referred to as individuals) undertake their legitimate duties in a manner compatible with the Data Protection Principles set out in the DPA 2018.

2. Scope

2.1 The procedures detailed below explain the core principles for the UK GDPR and DPA 2018 and how breaches must be reported and notified within each Force. In addition, containment and recovery options are provided with risk assessment options.

2.2 This policy must be read in conjunction with the DPA 2018 Breach Matrix and the wider policies dealing with data protection.

3. Policy Statement

3.1 Those processing personal data on behalf of the Forces are bound by the UK GDPR and DPA 2018. This policy will raise awareness of data breach cases to ensure that all individuals can identify a case and understand the steps required for dealing with them. It is also underpinned by procedures that set out minimum standards expected in protecting and safeguarding personal data. Breaches will be thoroughly investigated.

Procedure

1. Data Protection Act 2018 (DPA 2018)

1.1 The DPA 2018 is based around six principles of ‘good information handling’ and places certain obligations on the Forces when processing personal data. The DPA 2018 enshrines in law specific rights for the individuals whose personal data is being

processed and these rights extend to instances when their data is impacted by a data breach.

1.2 Anyone who processes personal data for or on behalf of the Forces is bound by the DPA 2018.

1.3 Processing data means obtaining, recording, holding and performing any operation on the personal / sensitive data, including the erasure / destruction of the data.

1.4 ‘Personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

1.5 The Data Controller for each Force is the respective Chief Constable.

1.6 A personal data breach means any accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.

1.7 There are various security measures in place to protect personal data processed on behalf of the Forces, however a breach may still occur e.g., from:

• Theft or loss of data or equipment on which data is stored

• Inappropriate access controls allowing unauthorised use

• Accidental loss

• Destruction of personal data

• Damage to personal data

• Equipment failure

• Unlawful disclosure of personal data to a third party

• Documents lost / found / sent to wrong destination

• Human error

• Unforeseen circumstances such as a fire or flood

• Cyber attack

• Phishing offences where information is obtained by deceiving the organisation who holds it.

1.8 Sussex Police also record breaches as notified by the Crown Prosecution Service (CPS), these are recorded as ‘Advisory Only’ and not breaches.

1.9 Refer to the Surrey Police and Sussex Police Information Security Policy (722) for further information on overarching protective security safeguarding the integrity availability, and confidentiality of the Force’s information and information systems.

2. Reporting

2.1 If you discover that data has been lost, or if you believe there has been a breach in the way that personal data is handled, you must immediately, or no later than within 24 hours of first coming to notice, inform the respective Force Data Protection Officer (DPO) via the reporting tool mentioned at Point 5.

2.2 They will follow the Information Commissioner's Office (ICO) guidelines on notification and recording a breach. Following this report to the DPO, you must also report to your supervisor / line manager. The priority must then be to manage the breach to mitigate / minimise the risks to those individuals affected by it.

2.3 When dealing with a data breach incident, the following points will need to be carefully considered, and the appropriate actions promptly carried out to minimise the impact of the data breach. The primary responsibility is to ‘protect the data subjects so a swift Threat, Harm, Risk, Investigation, Vulnerability, Engagement (THRIVE) risk assessment is essential. Then consider:

• Containment and recovery

• Assessment of on-going risk

• Notification of breach

• Evaluation and response

3. Containment and Recovery

3.1 The respective Information Management (IM) team / DPO working with the Security and Information Assurance Team (SIAT) will take appropriate steps to investigate and contain the situation. The DPO / IM will analyse and assess any risks to determine safeguarding needs and develop a recovery plan including damage limitation.

3.2 Specialists input from across the Forces such as Digital Data and Technology Department (DDaT), People Services, Media and Communications, legal and in some cases contact with external third parties may be required and will be determined on a case by case basis.

• The containment exercise could include isolating or closing a compromised section of the network, recovery of released documents, finding a lost piece of equipment, or simply changing any related access codes. The respective DPO must be informed.

• Establish whether there is anything you can do to recover any losses and limit the damage the breach can cause, such as sending an email to the wrong recipient. In support of the Security and Breach Reporting tool (SABR), you must recall the original email (if internal recipient, this does not work external emails), contact the incorrect recipient to delete all copies of the email and state that any further processing by them is unlawful.

• Recovery attempts can include the physical recovery of equipment, the use of backups to restore lost or damaged data or ensuring that individuals recognise when someone tries to use stolen data to access accounts.

3.3 On discovery of a data breach by any individual, immediate steps must be taken to minimise the damage caused by the breach and to prevent the breach from continuing.

4. Assessing the Risks

4.1 Level of breach risks can be very different depending on what is lost / damaged / stolen / unlawfully disclosed. The respective Force only needs to notify the ICO of a breach 'if it is likely to result in a risk to the rights and freedoms of individuals'. However, all breaches must be reported promptly to the respective DPO / team to make the decision on whether or not the ICO needs to be informed of the breach (breaches are also reported to the SIAT for Police Digital Services (PDS) reporting). Please refer to the DPA 2018 Breach Matrix which details the referral process.

4.2 Do not refer any breaches to the ICO, all referrals must come from the DPO or IM teams.

4.3 When making a decision on the risk that flows from a data breach the following points should be considered.

• What type of data is involved?

• Is the data likely to be placed in the public domain?

• Could the loss result in the data subject becoming a victim of crime?

• How sensitive is the data (i.e. what is the impact on the subject's privacy)?

• If data has been lost or stolen, are there any protections in place such as encryption?

• What has happened to the data?

• If data has been stolen, could it be used for purposes which are harmful to the individuals to whom the data relates? If it has been damaged, this poses a different type and level of risk.

• Regardless of what has happened to the data, what could the data tell a third party about the individual? Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people.

• How many individuals' personal data has been affected by the breach?

• Who are the individuals whose data has been breached?

• What harm can come to those individuals?

• Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life?

• Are there wider consequences to consider such as a risk to life?

• The loss of public confidence is as important to the service you provide.

5. Notification of Breaches

5.1 You must inform the respective DPO, SIAT Officer and your supervisor / line manager immediately on being aware of the breach. To report a breach, use the Security and Breach Reporting tool (SABR). A report must also be made to the IT Service Desk for IT related breaches. You may also need to inform the respective Force Professional Standards Department (PSD) if the breach is potentially as a result of an individual's misconduct.

5.2 The DPO / IM team may ask you additional questions about what has occurred and request the informant provides further answers not contained with the reporting tool in order to ascertain any further actions including whether the breach qualifies for immediate notification to the ICO or not.

5.3 The DPO needs to:

• Assess the type and level of risk and, if necessary, inform the ICO by phone as soon as possible and in any event within 72 hours of the breach being discovered;

• If a breach is likely to result in a high risk to the rights and freedoms of individuals, the DPO, or relevant business area if the DPO needs to remain impartial, must notify those concerned directly without undue delay;

• Confirm all the details and send completed form to the ICO.

5.4 The ICO, will investigate breach reports in their capacity as the independent regulator for Data Protection.

5.5 The IM teams manage the breach inbox during office hours (Monday to Friday, 0700 – 1600) and will monitor during bank holiday weekends.

5.6 If reporting a data breach out of hours, contact your respective Silver / Gold / Duty Commander. They will assess any immediate risks and recommend any immediate mitigating steps to protect potential victims (such as contacting IT to block lost mobile devices, contacting victims, if necessary, etc).

5.7 All breaches must be reported using the SABR Form to ensure this is logged with the IM team.

5.8 The DPA 2018 Breach Matrix can assist in any assessing any immediate risks if necessary.

5.9 Further information on breach reporting can be found on the How do I? Report a Data Security Breach.

6. Evaluation and Response

6.1 Following every incident of a personal data breach it is important to investigate causes to evaluate the effectiveness of the Forces response to it.

6.2 Simply containing the breach and continuing business as usual is not acceptable. You can discuss further prevention of breaches with the respective DPO and SIAT officer.

6.3 The IM team will review breaches to identify the need for training to support organisational learning.

6.4 Please contact the DPO via the following email address for more information

Surrey: dataprotection@surrey.police.uk or breach reporting dataprotectionbreaches@surrey.police.uk

Sussex: dpo@sussex.police.uk or Information.Management@sussex.police.uk

Team: Information Management