Data Protection Policy (Surrey and Sussex) (780/2022)

Abstract

This document outlines how the UK Data Protection Legislation and other enactments dealing with data protection, governs how personal data is processed in the UK (Data Protection Law) and applies to the Surrey Police and Sussex Police. Particular reference is paid to the general and security obligations which apply to the processing of personal data, disclosure obligations and exemptions and the specific responsibilities of the Data Protection Officer for both Forces. This policy should be read in conjunction with other Force polices that deal with data protection issues.

Policy

1. Introduction

1.1 The purpose of this policy is to ensure that all police officers, police staff and agents (including the extended police family of Special Constabulary, Police Community Support Officers (PCSOs), temporary staff, partner agency staff, consultants, contractors and volunteers) who work for Surrey Police and Sussex Police (hereafter referred to as the Forces) undertake their legitimate duties in a manner compatible with the Data Protection Principles set out in the Data Protection Act (DPA) 2018 and are clear about what is regarded as acceptable or proper use of personal data under existing Data Protection Laws.

1.2 The police process personal data for a policing purpose under Part 3 DPA 2018, or under UK GDPR for general processing. The DPA, 2018 supplements the EU General Data Protection Regulation (EU GDPR) in the UK Data Protection Legislation. The DPA, 2018 ensures a single, coherent, domestic regime for the processing of personal data for law enforcement purposes. Amongst other things, it regulates the use of information from which a living individual can be identified or is identifiable. It applies to the processing of personal data in most formats including electronic, paper and other media.

1.3 Key objectives are:

• All police officers / police staff process information lawfully in accordance with the DPA 2018.

• Individuals are protected from the use of inaccurate personal data.

• Individuals are protected from the misuse of accurate personal data.

• Personal data is safeguarded at every stage it is processed by the relevant Force.

• The Forces can demonstrate compliance with the requirements of the DPA 2018.

1.4 The DPA, 2018 requires every organisation that processes personal data to register with the Information Commissioner's Office (ICO), unless they are exempt. Failure to do so is a criminal offence.

• Surrey Police is registered and the reference number is Z4895085 which is renewed annually

• Sussex Police is registered and the reference number is Z5724254 which is renewed annually

2. Scope

2.1 This policy is underpinned by procedures that set out minimum standards and details how those employees (whether paid or unpaid) and any other authorised person having access to any Force data may lawfully use personal data held by the Forces. It also details the designation of the Data Protection Officer (DPO) and their specific responsibility to manage the statutory obligations of the Forces by ensuring compliance with the data protection principles and securing individual rights under the DPA 2018.

(Breaching this policy may result in disciplinary action for misconduct, including dismissal. Obtaining (including accessing) or disclosing personal data in breach of the Forces data protection policies may also be a criminal offence).

3. Policy Statement

3.1 Lawful processing of personal data is vital to the successful operation of the Forces and for maintaining the trust of the public and other stakeholders. The Forces are committed to protecting the rights and freedoms of individuals in accordance with the provisions of data protection legislation. In order to achieve this, the Forces shall ensure that personal data is handled appropriately and consistently. Both Forces' are committed to complying with the 6 data protection principles set out in the DPA, 2018.

3.2 The Forces may take criminal and/or disciplinary action against any category of person mentioned above whom wilfully accesses and/or misuses personal data held by either Force. Any use of personal data that does not have a clear policing or other statutory or business purpose is likely to constitute a misuse.

3.3 Section 170 of DPA 2018 identifies the following criminal offences for the unlawful obtaining, processing or retention of personal data:

It is an offence for a person knowingly or recklessly:

• To obtain or disclose personal data without the consent of the controller, or

• To procure the disclosure of personal data to another person without the consent of the controller, or

• After obtaining personal data to retain it without the consent of the person who was the controller in relation to the personal data when it was obtained.

3.4 Section 171 of the DPA 2018 states that it is an offence for a person to knowingly or recklessly re-identify information that is de-identified personal data without the consent of the controller responsible for de-identifying the person data.

3.5 Section 173 of DPA 2018 states that it is an offence for a controller or any person affiliated to the controller to alter, deface, block, erase, destroy or conceal information with the intention of preventing disclosure of all or part of the information that a person making a data access request would have been entitled to receive.

Procedure

1. Disclosure

1.1 There are instances where the information held by the Forces will need to be disclosed; the act of disclosing information is itself deemed as a form of processing personal data and will need to be done compliantly. Personal data held by the Forces is processed under the legislation outlined in policy section 1.2. In support of these purposes, relevant personal data can and should be shared with partner agencies to achieve crime prevention, investigation, detection, prosecution, safeguarding and implementation of judicial sanctions. This must always be done through a lawful authority, proportionately and in accordance with the Human Rights Act 1998.

1.2 The DPA 2018 provides additional rights for individuals in relation to their personal data. One such right is the right to access their personal data held by an organisation. Rights of Access Requests may be made either in writing or using the designated form or can be given verbally. For more information and access to the form please use the following links

(Surrey) Rights of Access

(Sussex) Rights of Access

If you are uncertain whether you have received a Rights of Access Request please contact the relevant Force Information Access Team immediately as responses need to be provided within 1 calendar month of the request being received. More information is provided within the Rights of Access Policy (Surrey and Sussex) (1181)

Rights of Access requests for the disclosures of any personal data are processed by trained decision makers in the Information Access Team who can be contacted via SubjectAccess@surrey.police.uk in Surrey and access1@sussex.police.uk in Sussex.

1.3 Regular sharing of information should be subject of an Information Sharing Protocol, Agreement or a Memorandum of Understanding in place detailing rules of those arrangements. Force employees should refer to the Information Management Policy (Surrey and Sussex) (1187).

1.4 The DPA 2018 provides exemptions that will enable the Forces to disclose special category data in circumstances without, for example, first obtaining consent. Where disclosure is in the vital interest of the data subject e.g. where there is a genuine life or

death situation (e.g. severe medical emergency or a potential suicide) there are provisions under the DPA 2018 which enable the necessary disclosure to be made. This exemption is set out in Schedule 8, paragraph 3 of the DPA 2018 and refers to the vital interests of the data subject.

1.5 The DPA 2018 provides an exemption for data controllers to disclose personal data that they would otherwise have been prevented from disclosing when it is necessary for the prevention or detection of crime and/or the apprehension of offenders. This enables either Force to request disclosure of personal data from other data controllers as part of the Forces policing function. When police are requesting information from a third party organisation or individual relating to an investigation, a Data Protection Request Form must be used. Please note that in Sussex, this request must be countersigned by an Inspector or equivalent if the information requested contains information about a vulnerable person or contains special category data.
It is a matter for the organisation from whom the personal data is sought to determine whether or not to disclose information, as there is no compulsion under the DPA 2018.

1.6 Police officers and police staff making use of this process should ensure that the events are adequately documented and retained pending any future challenge over possible unlawful processing of personal data, in accordance with Section 62 of the Act.

2. Request for police information

2.1 Other organisations may also request information from the police using the Data Protection Request Form.

2.2 It should be noted that there is no obligation for the Forces to comply with such a request and any disclosure must only be made in accordance with relevant Forces' duties, policies and/or prevailing legislation.

2.3 Each request must be considered on its individual circumstances and only relevant, proportionate and necessary disclosures made only where the considerations are satisfied. The receipt of such requests, together with the decision and any relevant responses, should be recorded and retained on the appropriate file and available for future audit or inspection.

2.4 In order to provide appropriate accountability, Sussex requests must be countersigned by an Inspector or equivalent if the information requested contains information about a vulnerable person or contains special category data.

3. Schedule 2 Part 1 Paragraph 5
Information required to be disclosed by law etc. or in connection with legal proceedings.

3.1 Schedule 2 Part 1 paragraph 5 of the DPA 2018 provides an exemption from some UK GDPR obligations which we could apply to allow us in certain circumstances to provide information necessary for the purpose of legal proceedings.

3.2 Please note there is no obligation for either Force to provide information and any disclosure must only be made in accordance with relevant Force policies and/or legislation.

3.3 Each request must be considered on its individual circumstances and disclosure made only where the relevant considerations are satisfied. The receipt of such requests, together with the decision and any relevant responses, should be recorded and retained on the appropriate file and available for any future audit or inspection.

3.4 Data Protection Guidance and forms are available on the respective Force website however any requests should be forwarded to the Information Access Team (Surrey via SubjectAccess@surrey.police.uk / Sussex via access1@sussex.police.uk) for review.

4. General Obligations under DPA 2018

4.1 The DPA 2018 requires the adoption of appropriate technical and organisational measures to implement the data protection principles and to safeguard individual rights (Section 57 DPA 2018). This is 'data protection by design and by default.' Essentially, the Forces are required to consider data protection and privacy issues upfront in everything they do.

Data Protection by design and default requires police forces to implement appropriate technical and organisational measures which are designed to implement data protection principles in an effective manner and to integrate into processing, safeguards which are necessary for that purpose.

The Forces will also ensure that, by default, only personal data which is necessary for each specific purpose is processed. Data Protection by default will influence the amount of personal data collected, the extent of its processing, the period of its storage and accessibility.

4.2 Data Protection Impact Assessments (DPIAs) are required when a type of processing is likely to result in a high risk to the rights and freedoms of individuals. The Forces adopt a system of screening questions to assess proposed processing, to determine risk and whether a full DPIA is required.

The Forces must, prior to processing, complete screening questions and a full DPIA where necessary. A full DPIA which will include a general description of the processing operations, assessment of the risks to the rights and freedoms of those data subjects and most importantly measures to mitigate those risks. Those measures will demonstrate compliance and take into account the rights and legitimate interests of the data subjects and other people concerned. Section 64, DPA 2018 applies. DPIAs will be completed by the business area that are changing / implementing processing and delivered through the project or change management risk processes.

4.3 DPIA Templates can be located via these links DPIA Questionnaire and DPIA Template. Not all new processing or activities require full DPIAs to be completed. If there are minor amendments to processes / activities the screening questions can be completed initially.

If a full DPIA is then required further advice will be provided by Information Management teams in both Forces.

5. Obligations Relating to Security under DPA 2018

5.1 Under Section 66, DPA 2018 the Forces must ensure they have in place appropriate technical and organisational measures which are implemented to ensure a level of security appropriate to the risks arising from processing personal data.

5.2 Data Protection breaches must be reported through the Security and Breach Reporting tool as soon as possible and in any case within 24 hours. Where a breach is reported, the Data Protection Officer (DPO) will review and, where appropriate, notify the breach to their supervisory authority (Information Commissioner's Office (ICO)) without delay and in any event within 72 hours.

5.3 Officers and staff who discover a data breach have a fast time duty to first contain that breach, minimise harm to data subjects and recover data as soon as possible. This will include establishing the nature of the data, volume and sensitivity, the risk it poses and to whom. Safety plans for those data subjects should also be considered. The management of potential harm is a business area responsibility; reporting and compliance with the legislation is led by the Forces Information management teams.

5.4 The data breach must be recorded and detail the facts relating to the breach, the effects and any remedial action taken to contain and reduce potential risks to data subjects.

5.5 If the notification to the supervisory authority is not made within 72 hours, the referral must be accompanied with the reasons for the delay in reporting the data breach which could also be subject to additional fines by the ICO for non-compliance with the DPA 2018. Section 67, DPA 2018 applies.

5.6 The ICO has powers to impose monetary fines up to 20 million Euros or 4% of a groups worldwide turnover (whichever is greater) on organisations regarding personal data / security breaches.

6. Obligations Relating to Personal Data Beaches

6.1 Please refer to the Data Protection Breach Policy (Surrey and Sussex) (1180) which sets out the Force's obligations in the event of a data breach.

7. Audit and Monitoring

7.1 To ensure compliance with the fifth principle under Section 39 of the DPA 2018, personal data processed for any of the law enforcement purposes cannot be retained longer than is necessary for the purpose collected. The Forces will only retain information in accordance with its published Retention Schedule which closely aligns with the National Police Chiefs' Council (NPCC) National Retention Schedule.

7.2 Compliance with the fifth principle will be audited to provide a systematic and independent examination to determine whether activities involving the processing of police information are carried out in accordance with each Force's policies and procedures and whether this processing meets the requirements of relevant legislation and standards.

8. Training

8.1 All police officers and police staff in both Forces are required to complete mandated College Learn (previously known as NCALT) training on Data Protection with annual refreshers.

9. Designation of a Data Protection Officer (DPO)

9.1 The respective Chief Constable will designate a DPO for each Force (Section 69, DPA 2018 applies). When designating a DPO, the controller must have regard to the professional qualities of the proposed officer.

9.2 The DPO acts on behalf of the relevant Chief Constable (Data Controller) to manage their statutory obligations in respect of DPA 2018, including notification of processing to the Information Commissioner; compliance with the data protection principles and securing the rights of individuals under the DPA 2018.

9.3 The relevant DPO has responsibility for:

• Monitoring and auditing the processing of personal data on all their Force information systems, in line with the NPCC Data Protection Manual of Guidance and other NPCC Guidance; and promoting awareness of data protection matters through training, policy development, advice and guidance, to assist both Force's and partnership agencies with the development of information-sharing protocols

• Investigating and resolving complaints made in relation to the handling of personal data and assisting, where appropriate, in the investigation of disciplinary and criminal matters relating to data protection

• Providing advice on DPIAs under Section 64, DPA 2018 and monitoring compliance where a type of processing is likely to result in a high risk to the rights and freedoms of individuals.

9.4 Further information relating to the role of DPO can be found on the intranet and Internet. If you wish to report any concerns or contact the DPO please do so via email dataprotection@surrey.police.uk / DPO@sussex.police.uk

10. Supporting Documents / Procedures

10.1 Legislation specifies that the Forces must be transparent with individuals regarding how we collect, use and retain personal data to provide clear and concise information about how we process their data. The Forces have multiple Privacy Notices, published internally and externally, that ensure compliance with this requirement.

Team: Information Management