Appropriate Policy Document –

Schedule 1, Part 4, Data Protection Act 2018

July 2018

Contents

Appendix A

Appropriate Policy Document – Schedule 1, Part 4, Data Protection Act 2018

1. Introduction

When processing personal data, Hereford & Worcester Fire and Rescue Service (the Service) will comply with the requirements of the EU General Data Protection Regulation 2016/679 (EU GDPR), the Data Protection Act 2018 (DPA) and any associated legislation.

The Data Protection Act 2018 outlines safeguards for processing special categories of personal data. This Appropriate Policy Document covers all processing of sensitive personal data by the Service as per DPA Schedule 1, when the following conditions are met:

- The data controller is processing personal data in relation to GDPR Articles 9[1] or 10[2]
- The data controller is relying on a condition listed in DPA Parts 1, 2 or 3 of Schedule 1[3]
- An Appropriate Policy Document is in place.

2. Relevant Schedule 1 conditions and data processing activities

The Service relies on DPA Schedule 1 conditions to process special categories of personal data, for example:

2.1 Conditions Relating to Employment, Health and Research, etc.

- Employment, social security and social protection
    - Processing personal data concerning health in connection with the Service's rights under employment law.
    - Processing data relating to criminal convictions in connection with the Service's rights under employment law in connection with recruitment, discipline or dismissal.
    - Providing human resources and occupational health facilities for employees.

2.2 Substantial Public Interest Conditions

- Statutory etc. and government purposes
    - Fulfilling the Service's obligations under the Fire and Rescue Services Act 2004 such as responding to emergencies, providing community safety advice.
    - Complying with other legal requirements, such as the requirement to disclose information in connection with legal proceedings.
- Equality of opportunity or treatment

[1] Processing of special categories of personal data
[2] Processing of personal data relating to criminal convictions and offences
[3] Special categories of personal data and criminal convictions etc. data

    - Ensuring compliance with the Service's obligations under legislation such as the Equality Act 2010 and Sex Discrimination Act 1970, including ensuring that the public sector equality duty is fulfilled when carrying out our duties.
- Preventing or detecting unlawful acts
    - Processing data concerning criminal records in connection with employment in order to reduce the risk to the Service and the community.
    - Carrying out enforcement action in connection with the Service's statutory duties.
- Protecting the public against dishonesty etc.
    - Processing data concerning criminal records in connection with employment in order to protect the local community.
    - Carrying out enforcement action in connection with the Service's statutory duties.
- Regulatory requirements relating to unlawful acts and dishonesty etc.
    - Complying with the Service's enforcement obligations under the Regulatory Reform (Fire Safety) Order 2005.
    - Assisting other authorities in connection with their regulatory requirements.
- Preventing fraud
    - Complying with the Service's enforcement obligations under the Regulatory Reform (Fire Safety) Order 2005.
    - Disclosing personal data in accordance with arrangements made by an anti-fraud organisation.
- Safeguarding of children and individuals at risk
    - Carrying out community risk assessments in order to identify households for targeted fire prevention visits.
    - Obtaining further support for children and individuals at risk by sharing information with relevant agencies.
- Safeguarding of economic well-being of certain individuals
    - Carrying out community risk assessments in order to identify households for targeted fire prevention visits.
- Occupational pensions
    - Fulfilling the Service's obligation to provide an occupational pension scheme.
    - Determining benefits payable to dependents of pension scheme members.
- Disclosure to elected representatives
    - Assisting elected representatives such as local government Councillors and Members of Parliament with requests for assistance on behalf of their constituents.

2.3 Additional Conditions Relating to Criminal Convictions, etc.

- Extension of conditions in Part 2 of Schedule 1 referring to substantial public interest.
    - The Service may process personal data relating to criminal convictions in connection with its enforcement obligations.

3. Securing compliance with Data Protection principles (GDPR Article 5)

In summary, Article 5[4] of the GDPR states that personal data shall be:

- processed lawfully, fairly and transparently
- collected for specific and legitimate purposes and processed in accordance with those purposes
- adequate, relevant and limited to what is necessary for the stated purposes
- accurate and, where necessary, kept up-to-date
- retained for no longer than necessary, and
- kept secure

In addition, Article 5 requires that the data controller is responsible for and can demonstrate compliance with the above principles (the accountability principle).

The Service has a Data Protection Officer who is accountable for ensuring the data protection principles are applied.

When processing special category data, the following procedures are used to ensure compliance with the data protection principles:

- processed lawfully, fairly and transparently
    - Provision of privacy notices
    - Compliance with conditions from both GDPR Article 6[5] and Article 9[6]
    - Use of data protection impact assessments to ensure proposed processing is carried out fairly
- collected for specific and legitimate purposes and processed in accordance with those purposes
    - Privacy notices set out the purposes for which personal data will be used
    - Personal data is not processed for other purposes without obtaining the data subject's consent unless authorised by law
- adequate, relevant and limited to what is necessary for the stated purposes
    - Use of data protection impact assessments to ensure that collected data is sufficient to provide the service but not excessive in order to protect individuals from harm.
    - Use of national guidance and relevant legislation to determine information that the Service should collect.
- accurate and, where necessary, kept up-to-date
    - Cross-matching data sets where possible to check accuracy

[4] Principles relating to processing of personal data
[5] Lawfulness of processing
[6] Processing of special categories of personal data

    - Review of personal information held when contacting individuals (data subjects).
    - Correction of personal data when notified of inaccuracies by data subjects as per GDPR Article 16[7].
- retained for no longer than necessary
    - Retention periods are set out in the Service's information asset register and privacy notices.
    - Retention periods are based on legal requirements to retain data and on Service standards.
- kept secure
    - The Service adheres to the Government's Minimum Cyber Security Standard and implements information security controls in line with ISO 27001.
    - The Service's Information Governance Forum meets regularly to ensure information security is maintained within the Service.
    - Service personnel are currently vetted in line with HMG Baseline Personnel Security Standard.
    - Technical security controls are employed to secure sensitive information.
    - Role-based access controls are implemented to restrict access to sensitive data.
    - Where possible, anonymization or pseudonymisation are used to reduce the risk of sensitive data being compromised.

4. Retention and Erasure of Personal Data

Personal data is held and disposed of in line with the Service's Information Asset and Retention Register (IARR). When disposing of information, the Service ensures this is carried out securely by using physical destruction methods as well as electronic data deletion.

The IARR contains details of the retention periods for the Service's data processing activities together with information on the lawful basis for processing this data.

5. Responsibility for Processing Sensitive Data

All employees are required to comply with the Service's Data Protection policies and Information Security Framework when processing sensitive / personal data to ensure that processing is carried out legally, fairly and transparently. Information Asset Owners are responsible for ensuring that systems and processes under their control comply with current data protection legislation and that personal data is processed in accordance with the data protection principles.

The Data Protection Officer will review this Appropriate Policy Document on a biannual basis to ensure that it remains current and relevant.

[7] Right to rectification

Appendix A

Definitions

Biometric data - personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a human being, which allow or confirm the unique identification of that person, such as facial images or fingerprints.

Consent of the data subject - any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Controller - the person, company, public authority (i.e. the Service), agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Protection Act 2018 – the current UK legislation governing data protection

Data Subject – an individual who is the subject of personal data

Filing system - any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

Genetic data - personal data relating to the inherited or acquired genetic characteristics of a human being which give unique information about the physiology or the health of that person and which result, in particular, from an analysis of a biological sample from the person in question.

Information Commissioner (ICO) – the UK's independent body responsible for monitoring the Data Protection Act, see www.ico.org.uk

Personal data - any information relating to an identified or identifiable human being ('data subject'). An identifiable human being is one who can be identified, directly or indirectly, in particular by reference to their:

- Name
- Address
- Telephone numbers
- Identification numbers, such as Payroll number, Service number or National Insurance number
- Recordings, photographs or reproductions of a person's voice, likeness or image
- Bank account numbers
- Medical records, attendance and sickness records
- Online identifiers (e.g. username or cookie).

or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

Special categories of personal data – this includes personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, and the processing of genetic data, biometric data for the purposes of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Personal data breach - a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Processing – data processing is the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data.

Processor - a person, company, public authority, agency or other body which processes personal data on behalf of the controller;

Profiling - any form of automated processing that evaluates personal aspects relating to a human being, in particular to analyse or predict aspects concerning that person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Pseudonymisation - the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable human being.

Recipient - a person, company, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.

Restriction of processing - the marking of stored personal data with the aim of limiting their processing in the future.

Third party - a person, company, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.