Appropriate Policy Document : Employment

Introduction

The Data Protection Act 2018 (DPA 2018) outlines the requirement for an Appropriate Policy Document (APD) to be in place when processing special category (SC) and criminal offence (CO) data under certain specified conditions.

Almost all of the substantial public interest conditions in Schedule 1 Part 2 of the DPA 2018, plus the condition for processing employment, social security and social protection data, require an APD to be in place. (See Schedule 1 paragraphs 1(1)(b) and 5).

This document demonstrates that the processing of SC and CO data based on these specific Schedule 1 conditions is compliant with the requirements of the General Data Protection Regulation (GDPR) Article 5 principles. In particular it should outline our retention policies with respect to this data. (See Schedule 1 Part 4).

If SC or CO data is processed for a number of different purposes a separate policy document for each condition or processing activity is not required – one document covers them all. Policies and procedures which are relevant to all the identified processing may be referenced. Whilst it is not necessary to explain compliance with the principles in general terms, without specific reference to each individual Schedule 1 condition you have listed, data subjects should be provided with sufficient information to understand how their SC or CO data is being processed and how long it will be retained for.

However, by relying on one of these conditions, the general record of processing activities under GDPR Article 30 must include:

(a) the condition which is relied upon;
(b) how the processing satisfies Article 6 of the GDPR (lawfulness of processing); and
(c) whether the personal data is retained and erased in accordance with the retention policies outlined in this APD, and if not, the reasons why these policies have not been followed.

The APD therefore complements NHPC's general record of processing under Article 30 of the GDPR and provides SC and CO data with further protection and accountability. See Schedule 1 Part 4 paragraph 41.

The APD must be kept under review, and it will be retained until six months after the date the relevant processing stops. If the Commissioner asks to see it, it must provide it free of charge. See Schedule 1 Part 4 paragraph 40.

This document should be read alongside the ICO Guide to the GDPR.

Description of data processed

Potential for SC/CO data to be processed when dealing with employment matters including Payroll, HR function and Recruitment

Schedule 1 condition for processing

Data Protection Act 2018, Schedule 1 (1) : Employment, social security and social protection

Procedures for ensuring compliance with the principles

Accountability principle

Do we maintain appropriate documentation of our processing activities?
Yes - comprehensive data mapping includes reference and information regarding Article 30

Do we have appropriate data protection policies?
Yes - Privacy Notice

Do we carry out data protection impact assessments (DPIA) for uses of personal data that are likely to result in high risk to individuals' interests?
Yes - not required

Principle (a): lawfulness, fairness and transparency

Have we identified an appropriate lawful basis for processing and a further Schedule 1 condition for processing SC/CO data?
Article 6(1)(b) - Contracts
Schedule 1 (1) - Employment, social security and social protection

Do we make appropriate privacy information available with respect to the SC/CO data?
There is the published Privacy Notice

Are we open and honest when we collect the SC/CO data and do we ensure we do not deceive or mislead people about its use?
Yes

Principle (b): purpose limitation

Have we clearly identified our purpose(s) for processing the SC/CO data?
1) The purpose is to meet obligations in relation to the employment of staff

Have we included appropriate details of these purposes in our privacy information for individuals?
Yes - full details are included in the published Privacy Notice

If we plan to use personal data for a new purpose (other than a legal obligation or function set out in law), do we check that this is compatible with our original purpose or get specific consent for the new purpose?
There are no plans to use the data for any other purpose

Principle (c): data minimisation

Are we satisfied that we only collect SC/CO personal data we actually need for our specified purposes?
Yes

Are we satisfied that we have sufficient SC/CO data to properly fulfil those purposes?
Yes

Do we periodically review this particular SC/CO data, and delete anything we don't need?
Yes - as per the Documents and Retention Policy

Principle (d): accuracy

Do **we have appropriate processes in place to check the accuracy of the SC/CO data we collect, and do we record the source of that data?**
The source of the data is the data subject and is therefore considered accurate

Do we have a process in place to identify when we need to keep the SC/CO data updated to properly fulfil our purpose, and do we update it as necessary?
The data relates directly to the Data Subject and they are expected to update on any changes to details

Do we have a policy or set of procedures which outline how we keep records of mistakes and opinions, how we deal with challenges to the accuracy of data and how we ensure compliance with the individual's right to rectification?
There is a Subject Access Request Policy which is to be reviewed annually

Principle (e): storage limitation

Do we carefully consider how long we keep the SC/CO data and can we justify this amount of time?
Retention has been considered and set out in the Document and Records Retention Policy

Do we regularly review our information and erase or anonymise this SC/CO data when we no longer need it?
Yes

Have we clearly identified any SC/CO data that we need to keep for public interest archiving, scientific or historical research, or statistical purposes?
NHPC does not retain this type of data

Principle (f): integrity and confidentiality (security)

Have we analysed the risks presented by our processing and used this to assess the appropriate level of security we need for this data?

Yes

Do we have an information security policy (or equivalent) regarding this SC/CO data and do we take steps to make sure the policy is implemented? Is it regularly reviewed?

Yes - the Council has an adopted Privacy Notice and all staff have undergone training in Data Protection

Have we put other technical measures or controls in place because of the circumstances and the type of SC/CO data we are processing?

Yes - both IT security (password/MFA) and physical security (locked cabinets)

Retention and erasure policies

As per the Documents Retention Policy

APD review date

Annually in March as part of the Council's consideration of compliance to allow completion of Assertion 10 on the AGAR