Annex C: data protection principles

The data protection principles for the general processing of data (ie under part 2 of the DPA) are those stated in the GDPR. However there are some differences in the principles applicable to Law Enforcement Processing under Part 3 and Intelligence Services Processing under Part 4.

For your ease of reference, we have reproduced each of them below. You should also refer to the ICO's guidance at www.ico.org.uk

- GDPR data protection principles
- Data Protection Act 2018 Part 3: Principles applicable to Law Enforcement Processing

GDPR data protection principles

Article 5

Principles relating to processing of personal data

1. Personal data shall be:

    1. processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

    2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

    3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

    4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

    5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data

Annex D: case studies

Fairness and transparency

Supermarket providing privacy information to customers

A supermarket holds information about its customers through its 'loyalty' card scheme, in-store CCTV and records of payments. The company does not normally disclose any information to third parties, for example for marketing purposes. However, it would do so if the information it held were relevant to a police investigation or in response to a court order, for example.

The supermarket or the card scheme operator should have given customers privacy information that provided an explanation, in general terms, of the sorts of circumstances in which it would share information about scheme members with a third party, such as the police.

If the supermarket discloses information about a particular scheme member to the police, it does not need to inform the individual of the disclosure if this would prejudice crime prevention.

Fairness and transparency

Sharing customer details with a credit reference agency

A mobile phone company intends to share details of customer accounts with a credit reference agency.

It must inform customers when they open an account that it will share information with credit reference agencies.

Credit reference agencies need to be able to link records to the correct individual, so the mobile phone company must ensure it is collecting adequate information to distinguish between individuals, for example dates of birth.

The organisations involved must have procedures to deal with complaints about the accuracy of the information they have shared.

Fairness and transparency; privacy information

Public sector bodies sharing data to provide a co-ordinated approach

Personal information is shared between two county councils and 19 relevant partner organisations in order to prevent social exclusion amongst young people who have been, or are at high risk of disengaging from education, employment or training. By sharing information the partner organisations can ensure a co-ordinated approach to identifying and contacting each young person to offer the most appropriate support to encourage them back in to education, work or training.

As part of developing their data sharing agreement, all the partners updated their privacy notices to include this new data sharing and agreed that each organisation would communicate this via their websites as well as in correspondence and conversations their staff have with the young people.

Fairness and transparency

Duty to process data fairly when carrying out research using shared data

A local university wants to conduct research into the academic performance of children from deprived family backgrounds in the local area. The university wants to identify the relevant children by finding out which ones are eligible for Pupil Premium. Therefore it decides to ask all local primary and secondary schools to share this personal data, as well as the relevant children's test results for the past three years.

The DPA contains various provisions that are intended to facilitate the processing of personal data for research purposes. However, there is no exemption from the general duty to process the data fairly. Data about families' income levels, or eligibility for benefits, may be inferred from the Pupil Premium status of a child. Parents and their children may well object to the disclosure of this data because they consider it sensitive and potentially stigmatising. Data about a child's academic performance could be considered equally sensitive.

Instead the school could identify eligible children on the researchers' behalf and contact their parents, explaining what the research is about, what data the researchers want. The school might wish to obtain parents' consent for the sharing of the data, but other lawful bases would be available to it.

Alternatively, the school could disclose an anonymous data set, or statistical information, to the researchers.

Data sharing agreement; accountability

Information sharing framework in healthcare

Healthcare partners in one county decided to develop an information sharing framework to standardise their sharing processes and encourage agencies to share personal data safely. The framework helped their staff to comply with data protection legislation by sharing information lawfully, securely and confidentially. As a result they were able to integrate service provision across the county and deliver better care outcomes for their residents. In a key step, partners brought together information governance leads to oversee the changes needed to develop the framework.

Main purposes of the framework were to ensure that:

- people only have to tell their story once and can expect a better service delivery;
- local people have clear guidance about how their information is shared (and in what circumstances their consent may need to be sought to share it);
- professionals have access to the information they need, when they need it, to support better outcomes for local people;
- good decision making is supported by an information sharing framework providing staff with clear direction; and
- unnecessary appointments and admissions can be avoided.

The principles of the framework were to:

a) identify the appropriate lawful basis for information sharing;
b) provide the basis for security of information and the legal requirements associated with information sharing;
c) address the need to develop and manage the use of Information Sharing Agreements (ISAs);
d) encourage flows of personal data and develop good practice across integrated teams;
e) provide the basis for county-wide processes which will monitor and review data flows; and information sharing between partner services;

f) protect partner organisations from unlawful use of personal data; and
g) reduce the need for individuals to repeat their story when receiving an integrated service.

KEY LEARNING FROM THE INTRODUCTION OF THE FRAMEWORK

- Staff need to be empowered to feel confident about sharing information between partners. Senior leaders need to be visible to give staff the confidence to share patient information.
- Internal culture needs to be supportive. The culture needs to be underpinned by strong values and ethos. It is essential that a learning culture is developed so that mistakes can be shared and learnt from rather than brushed aside. This learning includes developing formal training for all staff who were using an integrated care record, supported by the framework.
- Transparency needs to be established so that there is a collective understanding of how the data will be shared and by whom it will be shared. Staff need to have clarity around their roles and responsibilities and the benefits of sharing information.
- Need to develop a culture of appropriate sharing in plain English. Messages need to be simplified to avoid confusion and jargon needs to be reduced.

Lawful basis: legal obligation; fairness and transparency; individual rights

Data sharing required by law

A local authority is required by law to participate in a nationwide anti-fraud exercise that involves disclosing personal data about its employees to an anti–fraud body. The exercise is intended to detect local authority employees who are illegally claiming benefits that they are not entitled to.

Even though the sharing is required by law, the local authority should still inform any employees affected that data about them is going to be shared and should explain why this is taking place, unless this would prejudice proceedings.

The local authority should say what data items are going to be shared – names, addresses and National Insurance numbers - and provide the identity of the organisation they will be shared with.

There is no point in the local authority seeking employees' consent for the sharing because the law says the sharing can take place without consent. The local authority should also be clear with its employees that even if they object to the sharing, it will still take place.

The local authority should be prepared to investigate complaints from any employees who believe they have been treated unfairly because, for example, their records have been mixed up with those of an employee with the same name.

Lawful basis; special category data; fairness and transparency; accountability

Considerations in relation to a healthcare data sharing agreement

Relevant parts of the NHS and social services in a region share personal information with the region's police force to ensure that mental health service users who are in contact with the police are safeguarded and have access to appropriate specialist support.

The partner organisations have developed a data sharing agreement to support their joint mental health policy. Depending on the circumstances of each case, the lawful basis may be consent or a task carried out in the public

interest. The data sharing agreement clearly identifies the various pieces of legislation that each partner relies on to specify their public functions and the provisions they need to meet if relying on consent. As special category data is likely to be necessary for referrals, they have also identified Article 9 conditions. The data sharing agreement reminds all parties to maintain the rights and dignity of patients, their carers and families, involving them in risk assessments wherever possible whilst also ensuring their safety and that of others.

Data sharing agreement; accountability; information rights

Public sector bodies sharing data to provide a co-ordinated approach

Personal information is shared between two councils, their local schools and colleges, housing providers, relevant community organisations, the local job centres and careers service in order to identify young people who already have been, or are at high risk of, disengaging from education, employment or training. By sharing the information, the partner organisations can ensure a co-ordinated approach to providing the most appropriate support to the young person to encourage them back in to education, work or training.

The partners used a data sharing agreement to set out their purpose, lawful bases and the information to be shared. The agreement included a section on how to handle data subjects' rights, and agreed shared security standards; the partners also updated their privacy notices. To quality assure their agreement, they shared it with a regional group of data protection practitioners for feedback. A timescale was also set for the partners to regularly review the agreement to ensure it stayed up to date and fit for purpose.

Data sharing under the Digital Economy Act 2017 powers

Both Companies House (CH) and Her Majesty's Revenue and Customs (HMRC) collect annual accounts from businesses. The accounts contain key corporate and financial information related to the company, such as the names of company directors or financial reporting figures showing their profit and loss.

There is the opportunity, however, for the same company to file a different set of accounts to each of the two organisations. By filing inflated accounts at Companies House and lower figures at HMRC, they will simultaneously

increase their creditworthiness with financial institutions and wider government whilst also reducing tax liabilities.

Until 2018, restrictions on data sharing had prevented HMRC and Companies House from sharing company accounts for comparison. With the introduction of the Digital Economy Act 2017, however, a permissive legal gateway was provided to share information to combat fraud.

Prior to sharing information, Companies House and HMRC met to draw up the governance and processes:

- They would share information as a pilot.
- Both parties designed and agreed a data specification.
- They completed a data protection impact assessment to ensure they considered proportionality and fair processing.
- Both parties signed an information sharing agreement.

HMRC disclosed the first set of company accounts information to Companies House in October 2018 – the very first transfer of data under the Digital Economy Act powers.

The pilot sought to address the fraud problem through ten defined data analytics and compliance work streams, each one relating to a mode of behaviour indicating false account filing and fraudulent activity. For the first time the pilot utilised qualitative analysis to access and compare key words and phrases. Further to this, the pilot also utilised Companies House back office data to uncover previously hidden links between companies, combined for the first time with HMRC intelligence.

The data-sharing pilot identified £14.6m of savings, with a further £100.6m if the data share was embedded as business as usual. In addition, they identified over 3,500 sets of accounts as incorrect at Companies House, thereby improving the integrity of the data held on the register.