Fourth Data Protection Principle – Data accuracy

At a glance

- You should take all reasonable steps to ensure the personal data you handle is not incorrect or misleading as to any matter of fact.
- You may need to keep the personal data updated, although this will depend on what you are using it for.
- If you discover that personal data is incorrect or misleading, you must take reasonable steps to correct or erase it as soon as possible.
- You must carefully consider any challenges individuals make regarding the accuracy of their personal data.

Checklist

- We ensure the accuracy of any personal data we create.
- We have appropriate processes in place to check the accuracy of the data we collect, and we record the source of that data.
- We have a process in place to identify when we need to keep the data updated to properly fulfil our purpose, and we update it as necessary.
- If we need to keep a record of a mistake, we clearly identify it as a mistake.
- Our records clearly identify any matters of opinion, and where appropriate whose opinion it is and any relevant changes to the underlying facts.
- We comply with the individual's right to rectification and carefully consider any challenges to the accuracy of the personal data.
- As a matter of good practice, we keep a note of any challenges to the accuracy of the personal data.

In brief

What is the data accuracy principle?

The fourth data protection principle says:

> Personal data shall be accurate and, where necessary, kept up to date.

This is the second of three principles about data standards, along with data minimization and retention limitation.

There are clear links to section 14 of the DPA, which gives individuals the right to have inaccurate personal data corrected.

In practice, this means that you must:

- take reasonable steps to ensure the accuracy of any personal data;
- ensure that the source and status of personal data is clear;
- carefully consider any challenges to the accuracy of information; and
- consider whether it is necessary to periodically update the information.

When is personal data 'accurate' or 'inaccurate'?

The DPA defines the word "inaccurate" as follows:

> *"inaccurate", in relation to personal data, includes data that are misleading, incomplete or out of date.*

Whether information is accurate or not will be a matter of fact, and will usually be obvious.

You must always be clear about what you intend the record of the personal data to show. What you use it for

may affect whether it is accurate or not. For example, just because personal data has changed doesn't mean that a historical record is inaccurate – but you must be clear that it is a historical record.

Example

If an individual moves house from Bodden Town to West Bay a record saying that they currently live in Bodden Town will obviously be inaccurate. However a record saying that the individual once lived in Bodden Town remains accurate, even though they no longer live there.

Also bear in mind that section 14 of the DPA, you could be ordered to correct inaccuracy or incompleteness in personal data (or to delete inaccurate or incomplete personal data) you hold, if a complaint made by the relevant individual is upheld.

What about records of mistakes?

There is often confusion about whether it is appropriate to keep records of things that happened which should not have happened. Individuals understandably do not want their records to be tarnished by, for example, a penalty or other charge that was later cancelled or refunded.

However, you may legitimately need your records to accurately reflect the order of events – in this example, that a charge was imposed, but later cancelled or refunded. Keeping a record of the mistake and its correction might also be in the individual's best interests.

Example

A misdiagnosis of a medical condition continues to be held as part of a patient's medical records even after the diagnosis is corrected, because it is relevant for the purpose of explaining treatment given to the patient, or for other health problems.

It is acceptable to keep records of mistakes, provided those records are not misleading about the facts. You may need to add a note to make clear that a mistake was made.

If you do not act accordingly, and the individual makes a complaint to the Ombudsman, the latter may issue an order that the personal data be supplemented by a statement of facts. In reaching a decision the Ombudsman will consider the purposes for which the data is being processed. The statement may indicate the individual's view that the data is inaccurate.

When the Ombudsman is satisfied that personal data is inaccurate, she may require that third parties to

whom the data has been disclosed be notified that the data has been rectified, blocked, erased or destroyed, except if it is not reasonably practical to do so.

Example

An individual finds that, because of an error, their account with their existing energy supplier has been closed and an account opened with a new supplier. Understandably aggrieved, they believe the original account should be reinstated and no record kept of the unauthorised transfer. Although this reaction is understandable, if their existing supplier did close their account, and another supplier opened a new account, then records reflecting what actually happened will be accurate. In such cases it makes sense to ensure that the record clearly shows that an error occurred.

What about accuracy of opinions?

A record of an opinion is not necessarily inaccurate personal data just because the individual disagrees with it, or it is later proved to be wrong. Opinions are, by their very nature, subjective and not intended to record matters of fact.

However, in order to be accurate, your records must make clear that it is an opinion, and, where appropriate, whose opinion it is. If it becomes clear that an opinion was based on inaccurate data, you should also record this fact in order to ensure your records are not misleading.

Nonetheless, where appropriate the Ombudsman may order the rectification, blockage, erasure or destruction of expressions of opinion based on inaccurate personal data. [s.14(1)]

Example

An area of particular sensitivity is medical opinion, where doctors routinely record their opinions about possible diagnoses. It is often impossible to conclude with certainty, perhaps until time has passed or tests have been done, whether a patient is suffering from a particular condition. An initial diagnosis (which is an informed opinion) may prove to be incorrect after more extensive examination or further tests. However, if the patient's records reflect the doctor's diagnosis at the time, the records are not inaccurate, because they accurately reflect that doctor's opinion at a particular time. Moreover, the record of the doctor's initial diagnosis may help those treating the patient later, and in data protection terms is required in order to comply with the 'adequacy' element of the data minimization principle.

If an individual challenges the accuracy of an opinion, it is good practice to add a note recording the challenge

and the reasons behind it.

How much weight is actually placed on an opinion is likely to depend on the experience and reliability of the person whose opinion it is, and what they base their opinion on. An opinion formed during a brief meeting will probably be given less weight than one derived from considerable dealings with the individual. However, this is not really an issue of accuracy. Instead, you need to consider whether the personal data is "adequate" for your purposes, in line with the data minimization principle.

Note that some records which may appear to be opinions do not contain an opinion at all. For example, many financial institutions use credit scores to help them decide whether to provide credit. A credit score is a number that summarizes the historical credit information on a credit report and provides a numerical predictor of the risk involved in granting an individual credit. Credit scores are based on a statistical analysis of individuals' personal data, rather than on a subjective opinion about their creditworthiness. However, you must ensure the accuracy (and adequacy) of the underlying data.

Does personal data always have to be up to date?

This depends on what you use the information for. If you use the information for a purpose that relies on it remaining current, you should keep it up to date. For example, you should update your employee payroll records when there is a pay rise. Similarly, you should update your records for customers' changes of address so that goods are delivered to the correct location.

In other cases, it will be equally obvious that you do not need to update information. Indeed, in some cases it may be necessary to preserve inaccurate or incomplete personal data, for example as part of an audit or complaints handling record.

Example

An individual places a one-off order with an organisation. The organisation will probably have good reason to retain a record of the order for a certain period for accounting reasons and because of possible complaints. However, this does not mean that it has to regularly check that the customer is still living at the same address.

However, if an individual informs the organisation of a new address, it should update its records. And if a mailing is returned with the message 'not at this address' marked on the envelope – or any other information comes to light which suggests the address is no longer accurate – the organisation should delete the address from its database, unless there is a valid reason for keeping the inaccurate personal data.

Depending on the nature of the processing activity, and where there is a need to prevent inaccurate or outdated data from influencing future processing outcomes, it may also be warranted to keep a hash of the inaccurate personal data instead of the personal data itself in clear form. This will reflect the third (data

minimization) and fifth (storage limitation) data protection principles of the DPA

What steps do you need to take to ensure accuracy?

Where you use your own resources to compile personal data about an individual, you must make sure the information is correct. You should take particular care if the information could have serious implications for the individual. If, for example, you give an employee a pay increase on the basis of an annual increment and a performance bonus, then there is no excuse for getting the new salary figure wrong in your payroll records.

It may be impractical to check the accuracy of personal data someone else provides. In order to ensure that your records are not inaccurate or misleading in this case, you must:

- accurately record the information provided;
- accurately record the source of the information;
- take reasonable steps in the circumstances to ensure the accuracy of the information; and
- carefully consider any challenges to the accuracy of the information.

What is a 'reasonable step' will depend on the circumstances and, in particular, the nature of the personal data and what you will use it for. The more important it is that the personal data is accurate, the greater the effort you should put into ensuring its accuracy. So if you are using the data to make decisions that may significantly affect the individual concerned or others, you need to put more effort into ensuring accuracy. This may mean you have to get independent confirmation that the data is accurate. For example, employers may need to check the precise details of job applicants' education, qualifications and work experience if it is essential for that particular role, when they would need to obtain authoritative verification.

Example

An organisation recruiting a driver will want proof that the individuals they interview are entitled to drive the type of vehicle involved. The fact that an applicant states in his work history that he worked as a Father Christmas in a department store 20 years ago does not need to be checked for this particular job.

If your information source is someone you know to be reliable, or is a well-known organisation, it is usually reasonable to assume that they have given you accurate information. However, in some circumstances you need to double-check – for example if inaccurate information could have serious consequences, or if common sense suggests there may be a mistake.

Example

A business that is closing down recommends a member of staff to another organisation. Assuming the two employers know each other, it may be reasonable for the organisation to which the recommendation is made to accept assurances about the individual's work experience at face value. However, if a particular skill or qualification is needed for the new job role, the organisation needs to make appropriate checks.

Example

An individual sends an email to her mobile phone company requesting that it changes its records about her willingness to receive marketing material. The company amends its records accordingly without making any checks. However, when the customer emails again asking the company to send her bills to a new address, they carry out additional security checks before making the requested change.

Even if you originally took all reasonable steps to ensure the accuracy of the data, if you later get any new information which suggests it may be wrong or misleading, you should reconsider whether it is accurate and take steps to erase, update or correct it in light of that new information as soon as possible.

What should you do if an individual challenges the accuracy of their personal data?

If this happens, you should consider whether the information is accurate and, if it is not, you should delete or correct it unless it is necessary to preserve the information in its inaccurate state (e.g. as part of an audit or complaints handling record).

Individuals may complain to the Ombudsman who may order that inaccurate data be rectified, blocked, erased or destroyed.

You should rectify, block, erase or destroy inaccurate personal data without delay, in particular when ordered to do so by the Ombudsman following a complaint by an individual. This may include any expression of opinion that appears to the Ombudsman to be based on the inaccurate data.

Also remember that individuals are entitled to require that you cease processing their personal data, in general, for a specified purpose or in a specified manner.

It may be reasonable to erase the data in some cases. If an individual asks you to delete inaccurate data it is

therefore good practice to consider this request.

Relevant provisions

Data Protection Act (2021 Revision)

Schedule 1, part 1, paragraph 4: Fourth data protection principle – Data accuracy

Section 14: Rectification, blocking, erasure or destruction