Sovereign Security UK

Data Controller Policy

The Data Controller is the legal 'person' responsible for complying with the Data Protection Act.

On this note the data controller for Sovereign Security UK is Andy Clarkson.

Data Processor

When work is outsourced, which involves the contracting organisation in having access to personal data, there must be a suitable written contract in place, paying attention to security.

The Data Controller (Andy Clarkson) remains responsible for any breach of Data Protection brought about by the Data Processor.

Fair processing conditions

Schedule 2 of the Data Protection Act lays down six conditions, at least one of which must be met, for any use of personal data to be fair.

These are (in brief):

- With consent of the Data Subject
- If it is necessary for a contract involving the Data Subject
- To meet a legal obligation
- To protect the Data Subject's 'vital interests'
- In connection with government or other public functions
- In the Data Controller's 'legitimate interests' provided the Data Subject's interests are not infringed

Notification

Andy has to consider whether they are exempt from Notification. If they are not exempt, they have to Notify.

This means completing a form for the Information Commissioner and paying a fee of £35 a year.

The Notification form covers:

- The purposes for which personal data is held (from a standard list)

and for each purpose (again from standard lists):

- The types of Data Subject about whom data is held
- The types of information that are held
- The types of disclosure that are made
- Any transfers abroad

There is probably no need to mention the details of the organisation's Notification in the policy.

The notification entry has to be reviewed each year and may have to change if the organisation changes its processing in significant ways.

Subject access

Individuals have a right to know what information is being held about them.

The basic provision is that, in response to a valid request (including the fee, if required), the Data Controller (Andy Clarkson) must provide a permanent, intelligible copy of all the personal data about that Data Subject held at the time the application was made.

Andy Clarkson may negotiate with the Data Subject to provide a more limited range of data (or may choose to provide more), and certain data may be withheld.

This includes some third-party material, especially if any duty of confidentiality is owed to the third party, and limited amounts of other material. ("Third Party" means either that the data is about someone else, or someone else is the source.)

Confidentiality

Confidentiality applies to a much wider range of information than Data Protection. It may be better to have a separate Confidentiality Policy.

If confidentiality is included in the Data Protection policy, it must be made clear that they do not cover the same things.

Some of the things that are likely to be confidential, but may well not be subject to Data Protection, include:

- Information about the organisation (and its plans or finances, for example)
- Information about other organisations, since Data Protection only applies to information about individuals
- Information, which is not recorded, either on paper or electronically

Information held on paper, but in a sufficiently unstructured way that it does not meet the definition of a "relevant filing system" in the Data Protection Act

Understanding of confidentiality

It is important to set out who has access, to which data, for which purposes. Access in this case means not just by staff, but also by people outside the organisation.

Normally access will be defined on a "need to know" basis; no one should have access to information unless it is relevant to their work. This may be relaxed in the case of information which poses a low risk: for example, a list of business contacts may be made generally available, even if this means people having access who don't strictly need it.

Where risks can be specifically identified, it may be worth making provision in the policy: for example, in work with teenagers, discussing how much information will be shared with their parents.

The limits to confidentiality must also be set out. There will always be cases where the organisation feels it is right to break confidentiality, and there should be a procedure for deciding on a case-by-case basis whether this is appropriate.

Communication with Data Subjects

It is worth describing how clients, staff and other Data Subjects will be informed about confidentiality, so that there is minimal risk of them being surprised at any later stage to find out that who has information about them.

Communication with staff

It is worth describing how staff will be informed and trained in their responsibilities, and also what the procedure is if they have any questions about whether information should be disclosed, or access allowed.

Authorisation for disclosures not directly related to the reason why data is held

These fall into two main categories: those likely to be at the instigation, or in the interests, of the Data Subject, and those which are made in the course of official investigations.

For the first (such as a financial reference request from a bank), consent from the Data Subject is likely to be the normal authorisation. This consent should be recorded. For the second, it may be appropriate for the Data Subject not even to be informed; authorisation should be made at a senior level within your organisation.

Security

Security must not be confused with confidentiality. The latter is about defining what is allowed — setting the boundary; the former is about ensuring that the boundary is maintained. However, there must be a relationship between the two.

Like confidentiality, security is not wholly a Data Protection issue. Again, a separate policy may be preferable. The entries for business continuity and personal security below are those with least Data Protection relevance.

Setting security levels

The greater the consequences of a breach of confidentiality, the tighter the security should be. It may be worth defining broad security levels.

Security measures

For each confidentiality level it may be worth setting out the broad security measures to be followed, such as password protection, clear desk policy, entry control.

Business continuity

This would include backup procedures (both for data and for key staff availability) and emergency planning.

Specific risks

It may be worth setting out special precautions to be taken when information is in particularly risky situations, such as being worked on at home, with clients, at meetings, etc.

It may also be worth addressing “social engineering” where staff are tricked into giving away information. Tactics for dealing with persistent requests for information over the phone, for example, or tips on dealing with the various e-mail risks may be worth considering.

Common situations which may be worth mentioning include whether staff contact details may be given over the phone

Personal safety

A full security policy must also address personal safety of staff, including lone working.

End notes