Holst
WORKPLACE CULTURE

HOLST SUBJECT ACCESS REQUEST (SAR) POLICY

Holst is aware of its obligations as a Data Controller, with primary responsibility for, and a duty of care towards the personal data within its control.

Data Subjects whose personal data is held by Holst are entitled to ask Data Controllers:

- Whether the Data Controller is processing any personal data about that individual and, if so, to be given:-
- a description of the personal data;
- the purposes for which they are being processed; and
- information on any organisation to whom that personal data is being, or might be disclosed.
- to be told about the sources from which the Data Controller derived the information so long as those sources are available to the Controller; and
- For a copy of the information held, in response to a valid request to that effect.

FORM OF THE REQUEST

A request for Personal Data is a known as a Subject Access Request. However, it may not always be necessary to treat a request for information as a formal request under the General Data Protection legislation.

If the request for information is one which Holst would normally deal with within the normal course of business, e.g. a request for a copy of a statement by a bank customer, Holst will consider whether this is a formal subject access request under the DP Acts, or whether it can be managed as a 'business-as-usual' process.

Where the Controller treats the request as a formal Subject Access Request, the Controller is entitled to ask for a maximum fee of £5.95, in order to deal with the administrative steps involved in fulfilling the request.

Where the Controller charges this fee, we will do so as early as possible in the Request process.

In order to be valid, a Subject Access Request should be in writing, and should include sufficient information to identify the Data Subject to the Data Controller's satisfaction.

Holst will supply a Subject Access Request Form for the Data Subject to complete.

When these criteria are satisfied, the Subject Access Request is considered valid, and the forty day response period commences.

Holst will strive to respond to a valid request as quickly as possible, but nonetheless within this 40-day period.

COMMUNICATING WITH THE DATA SUBJECT

Holst will communicate directly with the Data Subject once a valid Subject Access Request has been received.

Rather than having to provide a copy of all data held by the Controller, this contact may help the Data Subject to specify the exact information he or she wishes to receive, thereby reducing both effort and the time and cost required to collate and provide the data being sought.

However, we acknowledge that, where the Data Subject is adamant that he or she wishes to receive a copy of everything the Data Controller holds about them, then we will fulfil a complete and exhaustive search of the computerised and manually-held data in the organisation.

SYSTEMS SEARCH

Unless there is a legitimate option to reduce the scope of the Request, a search of all databases and all relevant filing systems (manual files) which are relevant under the Acts will be carried out throughout the organisation, including email.

There is no obligation to search back-up files, on the basis that the data in back-up is a copy of the data already held either on the 'active' systems, or in archive.

Holst will organise the response to the Request by giving one individual the responsibility for issuing requests for information throughout the organisation and receiving all the returns. This co-ordinator role will normally fall to the Data Protection Officer, where one has been appointed.

The co-ordinator will then have the job of printing out all computerised information which has been returned to them by each department. They will also have received photocopies of all relevant manual files, and will therefore collate two sets of material – one of computer printouts and the other of photocopied manual files.

MANUAL FILES

The manual files which are relevant to the Acts are those which pass the conditions set out in the definition of a relevant filing system. The key criterion is whether the file in question forms part of a structured set. The set has to be structured by reference to the Requestor or characteristics relating to Requestor. If, for example, the manual files are organised in alphabetical name order, or by payroll number, they will form a structured set.

RESTRICTIONS FOLLOWING RECEIPT OF A REQUEST

Compliance with the DP Acts is not intended to interfere with the normal running of a Data Controller's business and following the receipt of a valid Request, we are permitted to make changes

to the requested information in the normal course of operation provided that no changes are made because of the Request itself; this applies even where the Data Controller would rather not release the information in its current form. This includes the correction of any incorrect data held as the principle is that the individual has a right to request the actual information held about them (whether or not it is accurate or correct).

THIRD PARTY DATA

Once the information has been collected, the Request co-ordinator will consider their obligations to other data subjects.

The co-ordinator will put themselves 'in the shoes' of the individual making the Subject Access Request. They have to read every single page of information to see whether it reveals the identity of any third party, when viewed from the perspective of the person making the Request. If the identity of a third party is already known to the Data Subject, then the data containing the information relating to the third party can be revealed to the Data Subject, because he/she is already aware of that information.

However, where the identity of a third party is not already known to the Data Subject in the context revealed by the documents, then the Request co-ordinator will consider whether the Request requires the disclosure of the information relating to the third party or whether it is possible to separate this information from the other information to be disclosed, for example, by blanking out (redacting) the name of the individual, or blanking out other identifying particulars or any other material, would be sufficient to disguise the identity of the third party from the Data Subject.

At this point, all other information which is likely to come into the hands of the Data Subject must be considered as well. If the identifying material can be blanked out with black marker pen and the rest of the information on that page can be handed over without revealing the identity of the third party, then this information will be included in fulfilling the Subject Access Request.

EXEMPTIONS

Some material is exempt from inclusion in the response to a Subject Access Request.

This includes the content of negotiations with the Data Subject. If the Data Controller is negotiating with the Data Subject at the time at which the Data Subject makes the Subject Access Request, the Data Controller does not have to reveal requested information if to do so would be likely to prejudice those negotiations. Once the negotiations are complete and have been put into effect, the whole file becomes subject to Subject Access in the normal way.

Emails are subject to Subject Access, as are archived computerised and manual data. It must be remembered that CCTV footage and tapes of telephone conversations will also be included within the scope of the Request, and must be searched on receipt of a Subject Access Request if the data subject so requires.

Other general exemptions to subject access are national security and the prevention or detection of crime, or the apprehension or prosecution of offenders.

Where the personal data contain health information, there is a duty on the Data Controller to consult an appropriate health professional before the information can be released to the Data Subject. This is to avoid disclosing information about adverse health conditions to a Data Subject where the disclosure may be harmful or distressing to the Data Subject or to another person.

This requirement does not apply where the Data Subject has already had access to the information, or where the Data Subject originally provided the information himself or herself.

We recognise that failure to respond to a Subject Access Request within the 40-day period gives rise to the ability of the individual to complain to the Office of the Data Protection Commissioner, and may well give rise to an investigation by the Commissioner.

In addition, failure to respond within 40 days will be a breach of the Eighth Data Protection Rule.

PERMANENT AND INTELLIGIBLE FORM

It is possible to do so, Holst to liaise with the Data Subject as to the form in which we hand over the information to the Data Subject.

The default position is that the Data Subject gets a hard copy of the information in a "permanent and intelligible format" (which may make it necessary for any internal codes released with the information to be explained), unless the supply of such a copy is not possible or would involve a disproportionate effort, or the Data Subject agrees otherwise. Any terms which are not intelligible without an explanation must be accompanied by an explanation (e.g. a Glossary of Terms).

Finally, once the response to the Subject Access Request has been finalised, the Request co-ordinator will make a full copy of the material to be retained for our own reference.

The copy of the requested material will be dispatched by secure, registered delivery, and we will seek timely confirmation from the Data Subject on receipt of the material.

These records will be used as reference material should, in the future, there is any dispute as to the content or timeliness of the response provided to the Data Subject.