ANNEXURE C

SUBJECT ACCESS REQUEST POLICY

Contents

1. Introduction

Policies and privacy laws in some countries give individuals whose data is processed by IHCL the right to access, correct, verify, and/or remove the Personal Information (PI) that IHCL is holding about them. In some jurisdictions, there may be a legal requirement for IHCL to respond to an Access Request within a specified period of time. It is therefore critical that requests from individuals for access to their information be handled promptly.

2. Purpose

The purpose of this procedure is to highlight various obligations and approach that support compliance with the access requests of data subject, applicable to IHCL in its role as Data Controller as well as Data Processor.

3. Applicability

This Instruction applies to all IHCL personnel, operating units, and wholly owned subsidiaries worldwide. The scope of personal data included within this policy is limited to Personal Data concerning the Data Subject which is provided either by the Data Subject itself or any other source.

4. Responsibilities

In order to comply with the Subject Access Request, IHCL will, in its capacity as a Data Controller inform the data subject about all its rights at the time of obtaining personal data.

In its capacity as a Data Processor, IHCL will respond to the request of the individuals/ data subjects only if it is driven by contractual agreement. However, IHCL will in all cases have the capability to develop interfaces to respond to the requests of the individual.

5. Subject Access Request Process Flow

5.1 Receipt of a formal request

Individuals or Data Subjects have the right to obtain confirmation as to whether personal data is being processed. If personal information is being processed, they are entitled to access the following information:

- reasons why their data is being processed;
- description of the personal data concerning them;
- anyone who has received or will receive their personal data;
- details of the origin of their data if it was not collected from them;
- period of storage of personal data and the criteria used to determine the period;
- provision of rectification or erasure;
- right to lodge a complaint with authority;
- logic of automated profiling performed on personal data (if any);
- details of any cross border transfers involved (if any)
- logic of automated profiling performed on personal data (if any);

The request must be in writing, however it may or may not refer specifically to the relevant section of regulation instead it may just include the words: 'I want to see what's on my personal file' or 'I want to see everything you have on me'.

5.2 Validate the identity of requester (data subject)

On receipt of a formal request, the Data Controller will validate the identity of the individual making the request. The following shall be considered for validation of the request:

- Do we have the complete identity of the requester?
- Are we clear about the nature/extent of the request?
- Do we have sufficient information to locate the requested data?

If the answer to all of the above is "yes" then IHCL Data Request handler (IDRH) <TBU>will acknowledge the request in writing. IHCL shall also make the data subject aware of the latest date by which the requester can expect a response i.e. 30 calendar days for response time from date of receipt in the firm.
If the answer to any of the above is" no" IHCL will to go back to the requester as soon as possible, in writing and ask them to fill in the gaps.

- Where the requester is not a current employee IDRH must obtain a proof of ID and address. Proof of ID should be their passport (personal details page) or photo card driving license;

- Where someone is making a request on behalf of the requester (such as a claims management company or a solicitor) IDRH <TBU> must obtain a copy of the authorization from the individual for them to make the request on their behalf and to receive the response. To be certain there are no issues with potential illegal disclosures, you should also contact the individual directly and obtain their confirmation – as well as requesting their proof of ID and address.

- The thirty day statutory period will not begin until we have received all the necessary information from the requester. Once we believe we have all the details we need, we should write back to the requester to confirm this and the calculated date for our response.

5.3 Validate the request

After validating the identity of the Data Subject, the request will be checked for duplicate/ repeated requests. In case the request found is excessive or repeated, IHCL can charge reasonable administrative fees to respond to the request. IDRH<tbu> shall ensure the following for validating a subject access request:

- The request must be in written format. It must be clear and specific. IHCL can ask the data subject to narrow down the request to make it more specific;
- The request should not affect the rights and freedom of others;
- The request should not have negative impact on national security, public security, defense or challenge any criminal conviction on the data subject ;
- If the request is very broad or generic "I want everything you have on me" then IHCL<TBH> shall be entitled to ask the data subject to narrow it down. Depending on the circumstances this may require IDRH to ask for specific individuals they may have had contact with, particular timeframes, whether there are particular

issues/circumstances the request may pertain to (performance reviews, tax advice, job application etc.).

5.4 Log the request

The IHCL data request handler (the team to which the SAR has been made) will log the request on Subject Access Request database for future reference.

5.5 Request for additional data (if required)

IHCL Data Request Handler may ask for sufficient additional information to help find the requested data if required.
The one month statutory period will not begins when the request is received.
If no data is found (i.e. guest), advise the person of this and, where possible, give reason why.

5.6 Respond to the request

The IHCL Data Request Handler (the team to which the SAR has been made) will look in the matter and contact support teams within IHCL and to clients (if required), to provide data to the data subject within the timelines defined in section 6.
IHCL will erase, rectify, complete, amend or accordingly act on the data pursuant to a justified request.
IHCL will also respond to the request in a readily intelligible form.
IHCL has the right to deny the request; however, the reasons of denial will be provided as a part of the response to the data requestor.

6. Compliance Timelines

IHCL will respond to all data subject request within one month of its receipt. If request is complex or IHCL receives a huge number of requests, they may extend timeline by<TBU>. However, IHCL will inform the data subject of this within one month of the receipt of the request and explain why the extension is necessary.

Where IHCL is not taking action in response to a request, it will explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.