INPDR Subject data rights Policy

File name: INPDR Subject data rights Policy

	Name	Title	Signature	Date
Author	Conan Donnelly	Registry Manager		6th March 2020
Reviewer				
Authoriser				

Effective Date	6th March 2020
Review Date	

Version	Date	Author	Changes
0.1	6th March 2020	Conan Donnelly	

Introduction.

A “data subject” is the natural person to whom any given personal data relates. “Personal data” is defined in the legislation as *“data relating to a living individual who can be identified either from the data or from the data in conjunction with other information in the possession of the data controller”.* It should be noted that this definition of personal data covers data relating to the business activities of sole traders.

Data subjects have a number of legal rights relating to the collection and uses of their personal data. The International Neimann Pick Disease Registry (INPDR) is committed to fully respecting and facilitating the exercise by data subjects of these rights.

INPDR is under a legal obligation to respond fully, accurately and in a timely way to requests from data subjects. To ensure proper compliance with this obligation, INPDR staff should immediately refer such requests to the Data Protection Officer. The Data Protection Officer will then establish whether INPDR or another entity is the data controller and what steps need to be taken to comply with the request.

Requests may not always be obviously expressed as being made pursuant to data protection legislation - if in any doubt, seek clarification from the Data Protection Officer, who will advise on how to deal with the matter.

A number of the rights have time limits associated with them - for example, a request for a copy of personal data must be complied with within 30 days. It should be noted that in each case, these time limits are maxima - the requests must be complied with as soon as may be. It is not open to the data controller to deliberately take longer than reasonably necessary to fulfil the request.

The Data Protection Officer will log all data subject requests received and the responses provided. This will allow INPDR to demonstrate its compliance with its obligations, as well as to monitor the associated effort and cost.

Data Subject Rights

1. Right to establish processing.

Data subjects have the right to be informed by a data controller whether any of their personal data is being processed by the controller. If such data is being processed, the data subject is entitled to be given a general description of the kinds of data being processed and the purposes for which it is being used. This kind of request does not involve providing an actual copy of the data.

The request must be in writing (which may include email). The maximum time allowed to comply with this kind of request is 21 days. No fee may be charged.

Under the GDPR, the right to establish processing is incorporated into the right of access to personal data.

2. Right of Access to personal data.

Data subjects have the right to a copy of any of their personal data being processed by a data controller. The copy must be provided in permanent and intelligible form. What this means may depend on the context - for example, one couldn't assume that a data subject would have the equipment and ability to open and read a spreadsheet file sent on a CD.

These requests must be in writing (including in electronic form, e.g., email). The maximum time allowed to comply with this kind of request is 30 days. The controller may take up to three months, if necessary on the basis of the complexity and number of requests. However, if taking longer than one month, the controller must advise the data subject of the delay and the reasons for it within one month of receiving the request. Under the GDPR, no fee may be charged unless the request is manifestly unfounded or excessive (in particular if it is repetitious), in which case a reasonable fee taking into account the costs of providing the requested data may be charged, or the request may be refused. In such cases, the onus will be on INPDR to demonstrate that the request is unfounded or excessive.

The GDPR will also require that in addition to a copy of their data, data subjects be provided with information including:

- the categories of data held about them;
- the purposes of processing;
- the entities or categories of entities with which the data may be shared (in particular if this may involve transfers outside of the European Economic Area);
- the expected data retention periods or criteria used to determine such periods;
- the existence of the rights to request rectification, erasure, or restriction of processing of personal data, or to object to the processing of the data;
- the existence of the right to complain to the Information Commissioner;
- where data is not obtained directly from the data subject, information about the source of the data;
- if applicable, details of any automated decisions, including profiling, made about the data subject and an explanation of the logic of such decisions as well as the significance and envisaged consequences for the data subject.

As a matter of best practice, INPDR will include the above details in the responses to any access requests received prior to the coming into effect of the GDPR.

INPDR is entitled to and will, in the interest of ensuring data is only released to persons entitled to receive it, seek reasonable proof of identity from the requesting data subject such as copies of photo ID, utility bills, etc.

Before data is released, it will be reviewed by the Data Protection Officer, to ensure accuracy and completeness and also to check whether the data contains references to third parties which may need to be redacted to protect their privacy rights.

There are very limited exemptions to the right of access to one's personal data. Exemptions which could be relevant for INPDR's purposes include:

- *Personal data consisting of an estimate of, or kept for the purpose of estimating, the amount of the liability of the data controller concerned on foot of a claim for the payment of a sum of money, whether in respect of damages or compensation, in any case in which the application of the section would be likely to prejudice the interests of the data controller in relation to the claim;*
- *Personal data in respect of which a claim of privilege could be maintained in proceedings in a court in relation to communications between a client and his professional legal advisers or between those advisers;*
- *Personal data that are back-up data.*
- *Where the request contains insufficient detail to locate the information required;*
- *Where the Data Subject previously waived his or her rights;*
- *Where the supply of a copy of the data is not possible or would involve disproportionate effort;*
- *For the protection of the fundamental rights and freedoms of a third party;*
- *Where the Data Controller has previously complied with an identical or similar request, unless, in the opinion of the Data Controller, a reasonable interval has elapsed since the previous request, having regard to the nature of the data, the purpose(s) for which it's processed and the frequency with which it changes.*

If there is any doubt as to whether the Data Subject has the mental capacity to give consent, the INPDR must refer to the Mental Capacity Act 2005. The mental capacity assessment and outcome must be recorded. If the Data Subject is assessed as lacking mental capacity to give consent, the record holder and/or the Caldicott Guardian will consider whether:

- Releasing the information would be lawful, seeking legal advice if necessary
- The applicant is acting in the best interests of the data subject

It should be borne in mind that while in the first instance it is for INPDR to judge whether to avail of any of the above exemptions, should it do so, it must be in a position to stand over and justify its decision if the Data Subject refers the matter to the ICO.

3. Prevention of processing likely to cause damage or distress

Data subjects have the right to request a data controller to cease processing of their personal data in circumstances where such processing is causing or is likely to cause substantial and unwarranted damage or distress to the data subject or another person.

The request must be in writing. The maximum time allowed to respond to this kind of request is 20 days. No fee may be charged.

The response must indicate whether the controller intends to comply with the request, in whole or in part. If the controller does not intend to comply, it must indicate why it considers the request to be unjustified.

Even if substantial and unwarranted damage or distress is likely, the data controller may still decline to comply with the request if:

- The data subject has given his or her explicit consent to the processing;
- The processing is necessary for the performance of a contract or the taking of steps with a view to entering into a contract;
- The processing is necessary for compliance with any legal obligation;
- The processing is necessary in the vital interests of the data subject.

4. Rectification, Erasure and Blocking.

Data subjects have the right to request a data controller to erase or block data (i.e., to flag it so that it may not be used for certain purposes, most commonly direct marketing) which was not fairly obtained or is not being fairly processed.

Data subjects have the right to request a data controller to rectify data relating to them which is inaccurate. The onus is on the data subject to provide the accurate data. Where data relating to this types of request has been disclosed to any other party within the 12 months preceding, the other parties must be notified within 30 days.

The request must be in writing (which may include email). The maximum time allowed to respond to this kind of request is 30 days. No fee may be charged.

5. Automated Decision Making.

Decisions which produce legal or other significant effects on data subjects may not be made solely by automated means. These include but are not limited to decisions relating to:

- Creditworthiness;
- Performance at work;
- Reliability;
- Conduct.

The right does not apply where the decision is in the data subject's favour. For example, if a credit card company scored all card applications automatically and approved all those above a given score, such decisions to approve applications would not be covered by this provision.

The data subject also has the right where automated decisions of any kind are being made about him or her to an explanation of the logic of the decision making process.

6. Prevention of processing for direct marketing.

Data subjects have the right to request a data controller not to process their data for direct marketing purposes. This is unlikely to affect INPDR's principal operations, but it should be noted that "direct marketing" is not necessarily confined to the sales and marketing of goods and services

on a commercial basis, but could include, for example, promotion by INPDR of informational events or activities.

Where the data is only being processed for direct marketing, it must also be erased in response to such a request.

7. Assistance from the Data Protection Commissioner.

Data subjects have a statutory entitlement to assistance from the Data Protection Commissioner. In privacy or data protection statements and in responding to requests this entitlement should be mentioned and data subjects should be advised that if they are dissatisfied with INPDR's response, they may refer the matter to the Commissioner.

8. Compensation.

Data subjects are entitled to take legal action to seek compensation for any loss or damage caused by a failure by INPDR to comply with its obligations under data protection legislation. Staff and management should be aware of the resulting financial risk which non-compliance with data protection obligations creates. It should also be noted that the GDPR will extend this right to cover "non-material" damage, e.g., embarrassment, distress, reputational harm, etc.

End of document