INPDR Engaging data processors policy

File name: Engaging Data Processors Policy

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

Effective Date	5th March 2020
Review Date	

Version	Date	Author	Changes
0.1	5th March	Conan Donnelly	

Introduction

A "data processor" is a person or organisation which processes personal data on behalf of the "data controller". The "data controller" is the person or organisation which controls the contents and use of a given set of personal data.

It should be noted that the term "data processor" doesn't encompass the directly employed staff of the controller. A data processor is, in effect, an outsourced service provider which has been contracted to carry out certain defined data processing tasks on behalf of the data controller. Examples would include secure document storage and destruction, data centres, call centres, etc.

For the controller/processor relationship to be properly established, it is a legal requirement that a written contract be in place. The contract must also include undertakings on the part of the processor that it will only process the personal data which is the subject of the service in accordance with the controller's instructions and that the processor will keep the data secure from unauthorised access, alteration, deletion or other unlawful processing. The controller is in turn legally obliged to take reasonable steps to ensure the processor fulfils its obligations to secure the data.

It is critically important for both parties that the controller/processor relationship is properly put in place. From the controller's point of view, it may have little or no recourse against a processor which has misused or failed to secure data if the appropriate contractual provisions aren't agreed. For its part, the data processor's sole direct obligation to the data subjects is the requirement to keep their data safe and secure. However, without an appropriate contract, it could be deemed to be a joint data controller, with the full spectrum of obligations which that entails.

Provisions to be covered in data processor contracts.

Under the terms of the Article 28 of the General Data Protection Regulation (GDPR), the processor contracts must include the following provisions, which must be included in INPDR's contracts with data processors it uses. Prior to the coming into effect of the GDPR, all existing data processors must be identified and their contracts must also be reviewed and amended as necessary to incorporate these provisions.

a) The subject and time frame of the contract;

(General description of the service to be provided and expected term, whether fixed, renewable, or indefinite.)

b) Guarantees to only process data in accordance with the data controller's documented instructions (including the location of processing, if this may be outside of the European Union) as to what processing is to be performed on the personal data which is covered by the contract.

(This should preferably also include objective measurable service levels and any applicable penalties, or indemnification of the data controller against any losses caused by a failure of the data processor to fulfil its obligations under the contract or the law. Depending on the size and financial strength of the data processor, INPDR may wish to require proof of appropriate insurance, so that such indemnities can be relied on.)

c) Disclosure to the data controller of any legally binding request for access to personal data, except where such disclosure is itself legally prohibited, and guarantees that the data processor will reject any such request which is non-legally binding;

d) Guarantees that only authorised persons with an appropriate commitment to confidentiality, such as through an employment contract, will have data access;

(This should include temporary or contract staff of the processor as well as permanent employees.)

c) Guarantees of information security;

d) Guarantees that sub-contractors will not be employed in fulfilling the contract without prior general or specific authorisation from INPDR, that any changes to sub-contractors will be notified in advance to allow INPDR the opportunity to object, and the data processor's contracts with sub-contractors will include the same data protection compliance guarantees as provided by the initial processor, who will be responsible for any compliance failures on the part of the sub-contractor;

(INPDR should always remain in control of who is processing data on its behalf and be able to satisfy itself as to their suitability and reliability.)

e) Obligations to assist INPDR in facilitating the exercise by data subjects of their rights;

(This should specify that time is of the essence, given the time limits which apply to the exercise of many of these rights.)

f) Obligations to assist INPDR in complying with its duties with regard to information security, notification of data breaches to the Data Protection Commissioner and to data subjects, and performance of data protection impact assessments and related consultations with the Data Protection Commissioner;

(With regard to data breaches, this should specify that time is of the essence, given time limits on the reporting of breaches.)

d) Specification for the return or destruction of the personal data at INPDR's choice on termination of the contract or as required in accordance with INPDR's data retention policy;

(Consider whether to require INPDR retains ownership of any hardware or storage media used.)

j) Obligation to provide all information necessary to demonstrate data protection compliance and to cooperate with INPDR with regard to its right to monitor or audit data processing;

(This obligation implies a corresponding need for the processor to have a thorough awareness of its obligations and appropriate policies and procedures implemented to ensure its compliance including the back up of patient data and disaster recovery protocols. INPDR should require processors to provide policies and procedures and, preferably, evidence of their effective implementation, prior to engaging their services. It should also be noted that processors must provide this information without necessarily waiting for INPDR to request it.)

k) Obligation to advise INPDR if in the processor's opinion any of INPDR's instructions infringe data protection laws.

(Strictly speaking, this is an obligation which the GDPR imposes directly on the processor and, as such, it does not have to be expressly stated in the contract. However, for clarity and to ensure expectations are fully stated, it would be good practice to include reference to it in the contract.)

End of document