NEC PRACTICE NOTE 3
APRIL 2018

Implementing the requirements of Regulation (EU) 2016/679 (General Data Protection Regulation)

The General Data Protection Regulation (GDPR) has a significant impact on the method of collecting and handling personal data. Article 28 requires certain information to be included in contracts which involve the processing of personal data, and this must be provided for on any contract including NEC contracts which include such a requirement. GDPR applies to a contract where one of the parties is established in the European Union (EU), and it is intended that it will also apply in the UK after it leaves the EU.

This note provides guidance on the information that needs to be included in an NEC contract which includes the processing of personal data as defined in the GDPR in order to comply with Article 28. It describes the requirements in relation to an NEC4 Engineering and Construction Contract (ECC), but equivalent clauses would be needed on other NEC contracts when applicable. Any processing of personal data must be carried out in accordance with other requirements of GDPR; this practice note does not extend to those requirements.

There are various sources of guidance on how to implement the requirements of GDPR, for example in the UK that provided by the Information Commissioner's Office. This note does not provide detailed guidance on the steps needed to comply with GDPR; it is intended only to set out the essential provisions that need to be included in NEC contracts. In addition to these specific provisions, the contract must set out details of the nature, scope and duration of the data processing.

The regulations define processing as performing an operation on personal data, whether on a computer or in paper form. In meeting the requirements of the standard contract – for example assessing Defined Cost or accepting a replacement key person – the *Client* will not be processing the *Contractor's* personal data. Whilst the *Client* or a consultant acting on its behalf will need to inspect the *Contractor's* records of personal data, that does not itself amount to processing. In these cases, no additional requirements need to be added to the contract to address the requirements of the GDPR. However, the *Client, Contractor* and Subcontractor will have to comply with any requirements of the GDPR that apply to their own internal operations.

If the contract does include requirements for the *Contractor* to process personal data of third parties, for example recording details of objections to a planning application, the *Client* needs to include in the contract with the *Contractor* the provisions required by the regulations. If a Subcontractor is processing the data on behalf of the *Contractor*, the *Contractor* must add equivalent provisions into the subcontract.

The GDPR applies to the security of personal data of a data subject, and refers to the controller, the processor and sub-processors. Under an ECC contract that requires the processing of personal data of a data subject by the *Contractor* on behalf of the *Client*, the controller will normally be the *Client*, the processor the *Contractor*, and the sub-processor will be a Subcontractor at any level in the supply chain. In some cases, it may be that the *Contractor* or a Subcontractor becomes a controller if they introduce a requirement for the processing of personal data by their suppliers which is not a flow through of requirements in their contract with the *Client*.

The following requirements must be included in relevant contracts:

- only act on the written instructions of the controller;
- ensure that people processing the data are subject to a duty of confidence;
- take appropriate measures to ensure the security of processing;
- only engage sub-processors with the prior consent of the controller and under a written contract;
- assist the controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;
- assist the controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- delete or return all personal data to the controller as requested at the end of the contract; and
- submit to audits and inspections, provide the controller with whatever information it needs to ensure that the controller and processor are meeting their obligations in respect of Article 28 of the GDPR, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

Some of these matters – the need for written instructions, consent to subcontracting – are inherent in all NEC contracts. However, the regulations introduce greater restrictions in the case of handling personal data than simply the need for all instructions to be in writing. They effectively prevent the processor from taking any action in relation to the data which is not given in writing. It is necessary, therefore to include all of these provisions within the contract.

These requirements are constraints on how the *Contractor* Provides the Works. These provisions should therefore be included within the Scope. The following example sets out how these can be provided for within the section of Scope dealing with data management.

 © nec 2017

EXAMPLE SCOPE ENTRY FOR THE ECC

Data management

1.1 The following terms used in this section of the Scope have the definitions given to them in the General Data Protection Regulation (EU) 2016/679 (GDPR).

(1) The Data is personal data.

(2) The *Client* is the controller.

(3) The *Contractor* is the processor.

1.2 The *Contractor* processes the Data only in accordance with the Scope and in compliance with the requirements of the GDPR.

1.3 The *Contractor* obtains written commitments to confidentiality from persons authorised to process the Data and requires them not to process the Data except in accordance with the Scope.

1.4 The *Contractor* implements technical and organisational measures to maintain a level of security of the Data appropriate to the risk presented by processing.

1.5 The *Contractor* includes in any subcontract which involves the processing of Data the same requirements for Data processing to those in this contract. Further sub-subcontracting which involves the processing of Data is not made without the agreement of the *Project Manager*.

1.6 The *Contractor* assists the *Client* by appropriate technical and organisational measures for the fulfilment of the *Client's* obligation under the GDPR.

1.7 In accordance with the instruction of the *Project Manager*, the *Contractor* deletes or returns the Data to the *Client* before the *defects date*.

1.8 The *Contractor* makes available to the *Project Manager* information necessary to demonstrate compliance with the requirements for processing the Data.

1.9 The *Contractor* assists in audits, including inspections, conducted by or on behalf of the *Client*.

1.10 The *Contractor* immediately informs the *Project Manager* if it believes that an instruction infringes the GDPR or data protection provisions of a Member of the European Union.

1.11 If instructed by the *Project Manager*, the *Contractor* assists the *Client* to ensure compliance with its obligations under the GDPR.