Exertis (UK) Ltd General Data Protection Regulation Statement

exertis

a DCC business

exertis.co.uk

The General Data Protection Regulation (GDPR) comes into effect on 25th May, 2018. The UK government published the Data Protection Bill in September 2017, which will implement and supplement the GDPR in the UK.

Exertis (UK) Ltd (Exertis) has been running a GDPR project to assess what and how we do things and to enhance our controls around personal data in preparation for the new legislation.

All defined terms in this GDPR Statement shall have the meaning ascribed to them under the GDPR.

Exertis will in some instances act as a data processor and on some occasions act as a data controller and/or joint data controller. To ensure that there is consistency with regard to the statements it makes in relation to GDPR and to reinforce that Exertis takes its obligations under the legislation very seriously, Exertis advises that:

A. When Exertis is acting as a **data processor**, Exertis will:

1. not process personal data except on instructions from the data controller; and
2. agree a data processing agreement with the relevant data controller;
3. use reasonable endeavours to assist any controller, whose personal data it is processing, in fulfilling its obligations to respond to requests from data subjects;
4. implement and maintain an information security programme;
5. ensure that people authorised to process personal data are subject to a duty of confidentiality;
6. co-operate with Supervisory Authorities;
7. inform the controller without undue delay after becoming aware of any personal data breach.
8. not sub contract processing activities without prior written authorisation from the relevant controller; and
9. put in place adequate processes to ensure that personal data is adequately protected if transferred outside the EU.

B. When Exertis is acting as a **data controller**, Exertis will:

1. process personal data in accordance with the principles and grounds for processing set out in the legislation;
2. provide the necessary information to data subjects when it collects personal data;
3. put in place processes and procedures to allow data subjects to exercise their data subject rights;
4. put in place suitable measures to safeguard data subject's rights where automated decision making is necessary;
5. embrace the concepts of privacy by design and default;
6. agree a data processor agreement with any processors;
7. co-operate with Supervisory Authorities;
8. implement and maintain an information security programme;
9. make all notifications required under the legislation upon becoming aware of any personal data breach which requires notification;
10. where required will carry out Data Protection Impact Assessments;
11. put in place adequate processes to ensure that personal data is adequately protected if transferred outside the EU.