

LW/KL/NSI 018 17

07 August 2017

To: All NSI Approved Companies and applicants

Dear Colleague,

THE GENERAL DATA PROTECTION REGULATION (GDPR)

The GDPR is a recently published EU Regulation, with some similarities to the existing Data Protection Act (DPA), but with particular emphasis on the processing of **personal data** by organisations such as yourselves.

We would like to increase awareness that the GDPR is already in force alongside the DPA, and compliance with the GDPR by the 25th May 2018 is mandatory.

What is personal data?

Personal data can be defined as any information relating to a natural person, the data subject, who can be directly or indirectly identified by the use of that data; for example, by their name, ID number, or online identifier such as an email address.

What difference does the GDPR make?

For organisations such as approved companies keeping HR records, customer lists and contact details, the new Regulation should make little practical difference. However, if you hold information that falls within the scope of the DPA, it will most likely fall within the scope of the GDPR and **you will therefore need to be compliant** with the Regulation.

The GDPR introduces further rights of the data subject, including the requirement for consent to be given to process data, and prompt reporting of data breaches to the Information Commissioner's Office (ICO) with large fines for non-compliance.

For further information on the GDPR, please refer to the ICO website:

<https://ico.org.uk/for-organisations/data-protection-reform/>

The ICO have produced a useful guidance document to help organisations prepare for the GDPR in 12 steps:

<https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf>

For a range of products and services providing further useful guidance and help towards GDPR compliance:

<https://www.itgovernance.co.uk/eu-gdpr>

What else must I do?

The DPA requires every data controller (e.g. organisation, sole trader) who is processing personal data to register with the ICO. This can be done on their website here:

<https://ico.org.uk/for-organisations/register/>

NSI take cyber security and data protection very seriously and we have put steps in place within our organisation to ensure we maintain secure and compliant systems. If you have any questions regarding NSI's position on GDPR compliance and cyber security, please do not hesitate to contact me directly.

Yours sincerely,



Laura Welford

Quality Manager

laura.welford@nsi.org.uk

01628 764865