



General Data Protection Regulation (GDPR) Policy

General Data Protection Regulation (GDPR) is an EU regulation to ensure data protection of EU citizens. All businesses operating within the EU member states must be compliant with the regulations or will face penalty.

GDPR was introduced following concerns by the public regarding how their private data was used. The GDPR addresses how information is collected, stored, and transferred by businesses.

This document outlines the measure CNS locums Ltd takes in processing data in accordance with Data Protection laws to ensure employees and business partners are satisfied with how we handle their confidential information.

CNS Locums Ltd will retain personal data for a certain length of time as required by law. All data will continue to be held and treated in accordance with this policy.

CNS Locums Ltd is a recruitment business, therefore may need to share staff personal information to third parties, such as trusted businesses in private and public services. When information is passed to third parties, they must respect the security of the personal data and treat the information in accordance with the law. To register candidates with CNS Locums Ltd, we will ask the candidates to send us specific information about themselves which we may be required to share when required by law to third parties such as the police or the home office. All candidates will need a DBS check which will return information of convictions, cautions, reprimands, or final warnings.

The following types of private data is protected but not limited to:

Identifiable data- Name, addresses, DOB, ID numbers, passport copies, email addresses, education certificate copies, biometric data, Sexual orientation, ethnic data, genetics, and health data.

Responsibilities:

Each employee has a responsibility to make sure that personal data and the assigned company confidential information is accurate, properly documented and handled according. They must also ensure that the local GDPR policy of the assigned hospital/clinics/offices where they are completing a shift is respected and all data are handled accordingly.

Confidential information in a physical format (Paper/USB) should not be removed from secure locations at the assigned hospitals/clinics or offices.

Data Breach:

Personal data breach can be due to a security breach by accidental or unlawful destruction, alteration, or disclosure. This may be a result of accidental or deliberate causes of action. CNS Locums Ltd has a duty to report this to the Information Commissions Office (ICO) within 72 hours of becoming aware. If the breach is highly likely to affect the rights or freedoms of the individual, then we also have a duty to inform them without delay. We must offer our support and advice to help the individuals from its effect.

CNS Locums Ltd has a right to complain to the Information Commissioners Office (ICO) and the UK supervisory authority for data protection issues if we are concerned that our data has been confidential data has been breached. However, we will always try to resolve the issue and rectify any concerns.

Clients' confidential information

CNS Locums Ltd employees must keep all information strictly confidential about the agency's business, service users, colleagues, and clients. They are not to discuss the affairs of the company with anybody unless there is a legal

requirement to do so. They are not to discuss or obtain confidential information about the company or their clients outside the scope of their role.

References:

Data Protection Act 2018.

The information commissions office website: <http://www.ico.gov.uk/>

Next review date: July 2024

-End document-