DigiSig Rail Group Ltd
www.digisig.co.uk

DigiSig Rail Group Ltd

Data Protection Policy

Doc No.	DRGL/D/2.3.7	
Version	**Description**	
1.0	Initial Issue	
Produced By: Michael Hickey	Signed: 	Date: 26/04/2022
Reviewed By: Russell Simpson	Signed: 	Date: 26/04/2022

Data Protection Policy

DRGL are committed to fulfilling our obligations under the Data Protection Act 2018 in line with the UK's implementation of the General Data Protection Regulation (GDPR).

DRGL will hold and process the data we collect relating to our employees in the course of their employment, for the purposes of administration and management and to aid compliance with the appropriate policies, procedures, laws and regulations.

Everyone responsible for using personal data has to follow strict rules called *data protection principles.* They must make sure the information is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage.

Employees are deemed, by accepting and signing the contract of employment, to have consented to this company processing electronically and manually held data about themselves, both during and after employment, for the purpose stated. They are also consenting to the transfer, storage and processing of such data by this company or by third parties acting on behalf of this company, either inside the European Economic Area, or in any other country in which we may operate. This company will treat all data as confidential and take all reasonable security measures to protect the data during processing, storage and transfer.

All employees who have access to data relating to the business of this company and its employees, will be expected to take adequate precautions to ensure confidentiality, so that neither the business or individuals are liable to prosecution, or that any data is disclosed which might cause distress or hardship to present, former or potential employees or Clients of this Company.

All IRSE assessing is carried out under the IRSE confidentiality policy as part of Licensing Procedure No 1.

DRGL ensure they achieve GDPR, Data Protection by completing the small business owners and sole traders report which is available on the Information Commissioner's Office website: -

ICO assessment for small business owners and sole traders | ICO

Information and Cyber Security

All DRGL hardware systems are installed with McAfee LiveSafe Premium Plus virus software which provides protection against cyber-attacks and hacking.

All DRGL Staff currently meet the requirements for competence laid out in the IRSE Signalling Principles Designer Licence (and Signalling Designer) unit 2.4 which also forms the basis for DRGL Information and Cyber Security Guidelines. Any DRGL staff member who hold competence in Signalling Principles Designer or Signalling Designer will continue to meet these guidelines in line with their licence competence. Any DRGL staff which do not have IRSE licence competence must adhere to the following which is in line with the IRSE relevant competencies for DRGL's business.

Ensure design requirements for communication and cyber security have been incorporated.

- *You ensure that appropriate account has been taken of security requirements, regulations, standards and government agency advice in the preparation and delivery of your designs.*
- *You ensure and confirm that required protocols for the use of software, hardware and transferable hardware to ensure cyber and communication security have been included in the design package.*
- *You ensure that all documentation you prepare has the appropriate security marking and that you follow the controls the marking requires.*

Examples may include:

- *Configuration control of software and data*
- *Use of appropriate security software*
- *Protection of passwords and access codes*
- *No use of unauthorised memory sticks, CD ROMS, USB drives, etc*
- *No connection of unauthorised personal computers/electronic devices/smart phones etc. to the system*
- *Use of two stage authentication*