



## Data Protection Policy

The person responsible for this policy is Mr Damian Hayes

### Policy

The General Data Protection Regulations 2018 focuses on looking after the privacy and enhancing the rights of the individual and based on the premise that consumer and data subjects (including employees) should have knowledge of what data is held about them, how it's held and how it's used.

It is our policy to ensure we only retain any personal information for as long as is necessary to fulfil the business purpose for which it was collected and as necessary to comply with our legal obligations, resolve disputes, and enforce our agreements. We prohibit all persons who use information, which relates to identifiable individuals such as clients and employees, from using such data in an unauthorised way.

### Employee data

Personal data provided by you will be held and processed both electronically and manually by the Company during or after your employment with the company in line with a legal basis for processing data depending on the type of data such as;

- Necessary for the performance of a contract (for bank details and other personal data for the purposes of paying an employee; providing and administering benefits such as pension, life insurance, permanent health insurance and medical insurance; undertaking performance appraisals and reviews; maintaining sickness and other absence records and taking decisions as to your fitness for work; providing references and information to future employers, and if necessary, governmental and quasigovernmental bodies for social security and other purposes, including the Inland Revenue)
- Compliance with a legal obligation (employee right to work in the UK documents)
- Compliance with employment law ([employee health, race or ethnicity data)

With your consent the company and any other company in the group may process Sensitive Personal Data at any time, whether before, during or after your employment, where the Sensitive Personal Data relates to the following:

- Racial or ethnic origin: any processing for the purposes of operating the Company's equal opportunity policy
- Your health: any processing for the purposes of operating the Company's sickness policy monitoring absence and any relevant pension scheme

01684 218 618 | [denovorisksolutions.co.uk](http://denovorisksolutions.co.uk)



- An offence committed, or allegedly committed, by you or any related proceedings: processing for the purpose of the Company's disciplinary procedures
- For all Sensitive Personal Data any processing in connection with a Change of Control of the Company or the transfer of any business in which you perform your duties or any after processing in the legitimate interest of the Company

You are required to provide the Company with the necessary information to update your personal records, i.e. change of name, address, marital status or number of children. In addition, periodically, the Company will send you the information held on its system in order that you may verify that it is accurate.

You have a right to know and ask: (a) whether your personal information is being processed, why and how and with whom it's shared; (b) about access to your data and to have inaccurate data rectified; and (c) us about your right to require us, as an employer to erase personal data about you in certain circumstances. Please refer to our Company's Employee Privacy Policy for further information

### **The General Data Protection Regulations 2018 ('The Regulations') and implications**

It has been and remains company policy to maintain high standards in the storage and use of personal data. These standards enable us to ensure client and employee confidentiality, as well as meet our obligations under the General Data Protection Regulations.

'Personal data' is '*any information related to a natural person or data subject that can be used to directly or indirectly identify a person.*' This may include name, a photo, a personal email address, bank details, post's on social media, location data, medical information or a computer IP address.

Personal data also includes any expression of opinion about an individual.

'Sensitive data' is '*personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation or biometric data.*'

Everyone's work involves the use of personal data and we must all be aware of and observe the requirements of The General Data Protection Regulations 2018. The Regulations include criminal offences for the companies, individual managers and employees if Data Protection law is breached.

The Regulations apply to all types of personal and sensitive data stored either on computers or in manual files. It requires every organisation or individual using personal data (the 'data controller') to notify the Information Commissioners Office of the purposes for which they hold data, the types of data held, the sources of data and the persons or organisations to whom data might be disclosed. An indication of our notification details is given below.

**01684 218 618 | [denovorisksolutions.co.uk](http://denovorisksolutions.co.uk)**



Data controllers are required to act in accordance with the six General Data Protection Regulation principles.

### **Our company's notification**

Our notification covers normal business activities for **all trading companies within the group**. So long as you are using personal data within an authorised work context you will be covered by the notification.

### **The six General Data Protection Regulation principles**

The Regulations requires personal data to:

1. Be processed lawfully, fairly and transparently
2. Collected for specified explicit and legitimate purposes
3. Adequate, relevant and limited to what's truly necessary
4. Accurate, kept up to date and every reasonable step to be taken to ensure that inaccurate data is deleted or rectified
5. Ensure identification of data subject is for no longer than necessary
6. Confirm appropriate protection measures are in place against unlawful or unauthorised processing, as well as accidental loss or destruction

### **Subject rights**

Any individual has the right to:

- Have their personal data erased
- Transfer their personal data to another service provider
- The rectification of inaccurate personal data without delay
- Receive transparent notices about how their data is used
- Access their personal data (subject access request) without charge and within one month of their request; and
- Where personal data is processed automatically, an outline of the logic involved in any decision making process

### Direct marketing

Direct marketing is a communication that promotes a product or service, including a website or mobile application that is sent directly to a specific business contact by post, telephone, email, or text message. Consent to direct marketing does not remain valid indefinitely.

### Right to object to automated decision taking

01684 218 618 | [denovorisksolutions.co.uk](http://denovorisksolutions.co.uk)



A data subject has the right to object to decisions taken by automated means in circumstances where the decision:

- Is taken by or on behalf of the Company
- Significantly affects that individual
- Is based solely on the processing by automatic means of the individual's personal data
- Is taken for the purpose of evaluating matters relating to them

Examples of areas likely to be affected are:

- **Personnel/HR**, where automated decisions may be taken, for example, in respect of absence from work due to illness or accident or an individual's performance at work
- Credit scoring, where an automated decision may be taken by reference to the data subject's credit worthiness

Subject rights – what to do if you receive a request

A data subject has the right to access personal data which has been collected about them. To do this they make a Data Subject Access Request (DSAR). We will accept a request by verbal, written or electronic means. Standard DSAR forms can make it easier for us to recognise a subject access request and make it easier for the individual to include all the details we might need to locate the information they want however we must make sure we tell a data subject that it is not compulsory for them to complete a DSAR form and we will not try to use this as a way of extending the one month time limit for responding. Individuals can obtain a standard DSAR form from the Information Commissioners Office website - <https://ico.org.uk>.

Requests from employees should be referred to **Damian Hayes**

All other requests, such as those from clients, will be handled by **Damian Hayes**

## **Your responsibility**

The General Data Protection Regulations carry penalties for individuals (as well as for companies) who breach the provisions. These are some areas you should consider.

## Use of Data

A Data Protection contact has been appointed within the business and given responsibility for handling queries relating to the use of personal and sensitive data, particularly in relation to new developments in the business and in systems. They will also review the use and storage of personal and sensitive data on a regular basis to ensure that data is used only in accordance with the company's notifications and the Principles.

**01684 218 618 | [denovorisksolutions.co.uk](http://denovorisksolutions.co.uk)**



Personal and sensitive data may be disclosed only as described in the Company's notification and in accordance with the Principles. Permissible disclosures are to:

- Managers and employees who need access to such data in order to fulfil the properly authorised requirement of their job
- Insurance companies for example in the context of broking a contract of insurance
- Anyone who has a legal right to demand it, for example the Department of Social Security, which has an overriding right to access personal data in many circumstances

Disclosure should only be made where we have told the individual who we may pass their details to and the reasons why.

Anyone in doubt about whether a particular disclosure is permitted should speak to Damian Hayes. Unauthorised disclosure will be treated by the Company as a disciplinary offence and may also be a criminal offence.

#### Overseas transfers of data

The Principles prohibit the transfer of personal data to countries outside the EEA unless certain criteria can be met.

#### Security

Appropriate measures must be taken to prevent unauthorised access to, disclosure of or damage to personal and sensitive data. Aspects to be considered include:

- Physical security of manual files, disks, tapes and printouts
- Secure placing and password protection of terminals and personal computers
- Security of laptop computers and mobile phones
- The reliability of colleagues, including careless talk outside the workplace

#### Legal Penalties

Contravention of the General Data Protection Regulations may lead to action by the Information Commissioners Office, who has wide-ranging powers to restrict the personal and sensitive data which the Company is permitted to hold and the purposes for which it can be used. Note also that criminal cases may be brought against individuals who handle personal and/or sensitive data in an unauthorised manner.

If a data subject suffers loss or damage because of unauthorised disclosure, inaccurate or missing data, or the loss or destruction of data, they may seek compensation in the Courts.

**01684 218 618 | [denovorisksolutions.co.uk](http://denovorisksolutions.co.uk)**



Do Novo Risk Solutions Ltd  
Office 3  
Raglan House  
Westminster Bank  
West Malvern  
WR14 4BN

### Further information

You can find further information about the General Data Protection Regulations from the Information Commissioners website <http://www.ico.gov.uk/> and you may wish to refer to the various guides issued in relation to the General Data Protection Regulations.

01684 218 618 | [denovorisksolutions.co.uk](http://denovorisksolutions.co.uk)

De Novo Risk Solutions Limited registered in England and Wales. Company Registration Number 10246240.  
Registered Office: Office 3, Raglan House, Westminster Bank, Malvern, WR14 4BN.  
De Novo Risk Solutions Limited are authorised and regulated by the Financial Conduct Authority (FCA),  
FCA Registration Number 786831. Our details can be checked by visiting the FCA's website: [www.fca.org.uk](http://www.fca.org.uk)  
or telephone the FCA on 0207 066 1000. We are covered by the Financial Ombudsman Service (FOS).  
Please see their website [www.financial-ombudsman.org.uk](http://www.financial-ombudsman.org.uk) for details and the Complaints section of our  
Terms and Business.

In association with  
**Bluefinnetwork**

