Data Protection under the General Data Protection Regulations (GDPR)

May 2018

	DATE	PREPARED	REVIEWED	REMARKS
ISSUE 1	17/05/18	HM	NS	-
REVISION 1	13/09/18	HM	NS	-
REVISION 2				
REVISION 3				

The Manse, 24 High Street,
Auchterarder, Perthshire,
PH3 1DF
T 01764 663839
info@nickisouterassociates.co.uk
www.nickisouterassociates.co.uk

Registered in Scotland.
Company No. : SC 377370

Introduction

The EU General Data Protection Regulation (GDPR) and the Data Protection Act (DPA) came into force on 25 May 2018, superseding the Data Protection Act 1998. GDPR will continue to apply despite Brexit, and impacts all organisations that control or process personal data. It grants data subjects a range of new rights, giving them more control over how their data is used. Organisations are subject to new responsibilities and obligations, including the need to demonstrate compliance.

Nicki Souter Associates (NSA) is committed to complying with the GDPR and DPA, and ensuring continuous improvement in information management across all formats. NSA strives to deliver the high standards of data protection which will allow our staff and clients to have confidence that their data is well managed.

This NSA Policy document has been prepared to ensure that our employees and consultants are fully aware of the new obligations that GDPR and DPA introduced, and to ensure that there is accountability and shared responsibility for ensuring compliance, from Board level down and across the Company.

As part of staff induction all NSAL employees and subcontractors will be given face to face training, tailored specifically to job role.

In the course of your work with our Company you are likely to collect, use, transfer or store personal information about employees, clients, customers and suppliers, for example their names and home addresses. The UK's data protection legislation, including the GDPR contains strict principles and legal conditions which must be followed before and during any processing of any personal information.

The purpose of this policy is to ensure that you are aware that everyone has a responsibility to comply with the principles and legal conditions provided by the data protection legislation, including the GDPR and failure to meet those responsibilities are likely to lead to serious consequences. Firstly, a serious breach of data protection is likely to be a disciplinary offence and will be dealt with under the Company's disciplinary procedure. If you access another employee's personnel records or any sensitive personal information without authority, this will constitute a gross misconduct offence and could lead to your summary dismissal. Additionally, if you knowingly or recklessly disclose personal data in breach of the data protection legislation, including the GDPR you may be held personally criminally accountable for any such breach.

Breach of the data protection legislation, including the GDPR rules can cause distress to the individuals affected by the breach and is likely to leave the Company at risk of serious financial consequences.

If you are in any doubt about what you can or cannot disclose and to whom, do not disclose the personal information until you have sought further advice from the Company's Director – Nicki Souter or Data Representative – Jayne Mitchell

This policy does not form part of a contract of employment. However, it is mandatory that all

employees, workers or contractors must read, understand and comply with the content of this policy and you must attend associated training relating to its content and operation. Failure to adhere to this policy is likely to be regarded as a serious disciplinary matter and will be dealt with under the Company's disciplinary rules and procedures.

Definitions

Data Subject: a living individual.

Data Controller: the person or organisation that determines the means and the purpose of processing the personal data.

Data Protection Legislation: includes (i) the Data Protection Act 2018, (ii) the General Data Protection Regulation (EU) 2016/679) (GDPR) and any national implementing laws, regulations and secondary legislation, for so long as the GDPR is effective in the UK, and (iii) any successor and supplemental legislation to the Data Protection Act 1998 and the GDPR, in particular the Data Protection Bill 2017-2019 and the E-Privacy Directive (and its proposed replacement), once it becomes law.

Personal data: is any information that identifies a living individual (data subject) either directly or indirectly. This also includes special categories of personal data. Personal data does not include data which is entirely anonymous or the identity has been permanently removed making it impossible to link back to the data subject.

Processing: is any activity relating to personal data which can include collecting, recording, storing, amending, disclosing, transferring, retrieving, using or destruction.

Special categories of personal data: this includes any personal data which reveals a data subject's, ethnic origin, political opinions, religious and philosophical beliefs, trade union membership, genetic, biometric or health data, sex life and sexual orientation.

Criminal records data: means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

What are the GDPR principles?

We are a data controller. This means that we are required by law to ensure that everyone who processes personal data and special categories of personal data during the course of their work with us does so in accordance with the data protection legislation, including the GDPR principles. In brief, the principles say that:

- Personal data must be processed in a lawful, fair and transparent way.
- The purpose for which the personal information is collected must be specific, explicit and legitimate.
- The collected personal data must be adequate and relevant to meet the identified purpose.
- The information must be accurate and kept up to date.
- The personal data should not be kept in a form which permits identification of a data subject for longer than is necessary for the purposes for which it is used.
- The personal data must be kept confidential and secure and only processed by authorised personnel.

Other rules under the GDPR state that:

- The transfer of personal data to a country or organisation outside the EEA should only take place if appropriate measures are in place to protect the security of that data.
- The data subject must be permitted to exercise their rights in relation to their personal data.

The Company and all employees must comply with these principles and rules at all times in their information-handling practices. We are committed to ensuring that these principles and rules are followed, as we take the security and protection of data very seriously.

You must inform us immediately if you become aware that any of these principles or rules have been breached or are likely to be breached.

What are the lawful reasons under which we would expect you to process personal data?

Whilst carrying out your work activities you are likely to process personal data. The Company will only expect you to process personal data where the business has a lawful basis (or bases) to process that information. The lawful basis may be any one of the following reasons or a combination of:

a) Consent has been obtained from the data subject to process their personal data for specified purposes.
b) Where we need to perform the contract we have entered into with the data subject either for employment or commercial purposes.
c) Where we need to comply with a legal obligation.
d) Where it is necessary for our legitimate interests (or those of a third party) and the interests and fundamental rights of the data subject do not override those interests.

There are other rare occasions where you may need to process the data subjects personal information, these include:

e) Where we need to protect the data subject's interests (or someone else's interests).
f) Where it is needed in the public interest [or for official purposes].

You must always ensure that you keep a documentary inventory of the legal basis (or bases) which is being relied on in respect of each processing activity which you perform.

Privacy Notices

- Personal data must be processed in a lawful, fair and transparent way.

Before you begin collecting or processing personal data directly from a data subject you must ensure that an appropriate privacy notice has been issued to the data subject. Different notices are used for employment and commercial purposes. The content of the privacy notice must provide accurate, transparent and unambiguous details of the lawful and fair reason for why we are processing the data. It must also explain how, when and for how long we propose to process the data subjects personal information. We need to include information around the data subjects' rights and most importantly, the notice should also explain how we will keep the information secure and protected against unauthorised use.

Where you intend to collect data indirectly from a third party or a public source (i.e. electoral register), you must ensure that a privacy notice is issued to the data subject within a reasonable of period of obtaining the personal data and no later than one month; if the data is used to communicate with the individual, at the latest, when the first communication takes place; or if disclosure to someone else is envisaged, at the latest, when the data is disclosed.

You must only use data collected indirectly if you have evidence that it has been collected in accordance with the GDPR principles.

In all circumstances you must check that you are using an up to date version of the Company's privacy notice and it is being used in accordance with the Company's guidelines.

Purpose Limitation

- The purpose for which the personal information is collected must be specific, explicit and legitimate.

When you collect personal information you will set out in the privacy notice how that information will be used. If it becomes necessary to use that information for a reason other than the reason which you have previously identified you must usually stop processing that information. However, in limited circumstances you can continue to process the information provided that your new reason for processing the personal information remains compatible with your original lawful purpose (unless your original lawful basis was consent)..

Adequate and relevant

- The collected personal data must be adequate and relevant to meet the identified purpose.

You must only process personal data where you have been authorised to do so because it relates to your work or you have been delegated temporary responsibility to process the information. You must not collect, store or use unnecessary personal data and you must ensure that personal data is deleted, erased or removed within the Company's retention guidelines. You must not process or use personal data for non-work related purposes.

The Company will review its records and in particular employees' personnel files on a regular basis to ensure they do not contain a backlog of out-of-date or irrelevant information and to check there are lawful reasons requiring information to continue to be held.

Accurate and kept up to date

- The information must be accurate and kept up to date.

If your personal information changes, for example you change address or you get married and change your surname, you must inform your line manager as soon as practicable so that the Company's records can be updated. The Company will not be responsible for any inaccurate personal data held on its systems where you have failed to notify it of the relevant change in circumstances.

Kept for longer than is necessary

- The personal data should not be kept in a form which permits identification of a data subject for longer than is necessary for the purposes for which it is used.

Different categories of personal data will be retained for different periods of time, depending on legal, operational and financial requirements. Any data which the Company decides it does not need to hold for a particular period of time will be destroyed in accordance with its retention of data policy.

Kept confidential and secure

- The personal data must be kept confidential and secure and only processed by authorised personnel.

To achieve this you must follow these steps:

- The Company has in place appropriate technical and organisational measures to protect against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to data. These procedures must always be adhered to and not overridden or ignored.
- Where the Company provides you with code words or passwords to be used before releasing personal information, for example by telephone, you must strictly follow the Company's requirements in this regard.
- Only transmit personal information between locations by fax or e-mail if a secure network is in place, for example, a confidential fax machine or encryption is used for e-mail.
- Ensure that any personal data which you hold is kept securely, either in a locked filing cabinet or, if it is computerised, it is password protected so that it is protected from unintended destruction or change and is not seen by unauthorised persons.
- Do not access another employee's records without authority as this will be treated as gross misconduct and it is also a criminal offence.
- Do not write down (in electronic or hard copy form) opinions or facts concerning a data subject which would be inappropriate to share with that data subject.
- Do not remove personal information from the workplace with the intention of processing it elsewhere unless this is necessary to enable you to carry out your job duties and has been authorised by your line manager.
- Ensure that when working on personal information as part of your job duties when away from your workplace and with the authorisation of your line manager, you continue to observe the

terms of this policy and the data protection legislation, in particular in matters of data security.

- Ensure that hard copy personal information is disposed of securely, for example cross-shredded.
- Manual personnel files and data subject files are confidential and are stored in locked filing cabinets]. Only authorised employees have access to these files. These will not be removed from their normal place of storage without good reason.
- Data stored on memory sticks, discs, portable hard drives or other removable storage media is kept in locked filing cabinets.
- Data held on computers are stored confidentially by means of password protection.
- The Company has network back-up procedures to ensure that data on computers cannot be accidentally lost or destroyed.

Transfer to another country

- Transfer of personal data to countries or organisations outside of the EEA should only take place if appropriate measures are in place to protect the security of that data.

We do not generally have a need to transfer data outside of the European Economic Area (EEA). However, if you are requested to transfer personal data to a country or organisation outside of the EEA you must not transfer personal data to a country or organisation unless that country or organisation ensures an adequate level of protection in relation to the processing of personal data and you have in place safeguards to ensure this is done. Nicki Souter the Company Director or Jayne Mitchell, Data Representative before you send personal data outside of the EEA.

The data subject rights

- The data subject must be permitted to exercise their rights in relation to their personal data.

Under the GDPR, subject to certain legal limitations, data subjects have available a number of legal rights regarding how their personal data is processed. At any time a data subject can request that the Company should take any of the following actions, subject to certain legal limitations, with regard to their personal data:

- Allow access to the personal data
- Request corrections to be made to data
- Request erasure of data
- Object to the processing of data
- Request that processing restrictions be put in place
- Request a transfer of personal data
- Object to automated decision making

- Right to be notified of a data security breach

There are different rules and timeframes that apply to each of these rights. You must follow the Company's policies and procedures whenever you process or receive a request in relation to any of the above rights.

How should you respond to a data subject request?

You must follow the Company's data subject access procedure which details how to deal with requests and it describes the circumstances where a fee may be charged. The procedure includes the following:

- Always verify the identity of the person making a data subject request and the legitimacy of the request.
- If you are unsure as to whether you are authorised to action the request check the privacy notice to ascertain who is authorised to deal with data subject requests. If you are still unsure how to handle the enquiry, you should forward this to Nicki Souter the Company Director or Jayne Mitchell, Data Representative.
- If you are authorised to deal with the request do not give out confidential personal information unless you have received the appropriate consent from the data subject. Seek explicit written consent to process the data subject request and ensure that you keep a clear audit trail of the request and your response.
- Do not share personal information with a third party, unless the data subject has given their explicit prior consent to the sharing of their information. A third party is anyone who is not the actual data subject and can include a family member of the data subject.
- Take great care not to accidentally share information with an unauthorised third party.

Be aware that those seeking information sometimes use deception in order to gain access to it.

Categories of information

During the course of your employment you may be required to process personal data which falls into different categories, general personal data and special categories of personal data. All data should be processed in accordance with the privacy notice and at all times in a confidential manner. However, where that data is classed as a special category extra care should be taken to ensure the privacy and security of that data. This means that you should maintain a high level of security and you should only share this data with those who are also authorised to process that data. In the context of employee relations the scenarios when you may be required to process special categories information may arise for one or more of the following reasons:

- In order to comply with employment and other laws when processing and managing situations connected with absences arising in relation to sickness or family/ dependant related leave.

- To ensure health and safety obligations and other employment related obligations are met you may be required to process information about the physical or mental health or disability status of an employee in order to assess their capability to perform a role. You may also be required to monitor and manage sickness absence, recommend appropriate workplace adjustments and administer health related benefits.

- Where it is needed in the public interest, for example for equal opportunity monitoring and reporting.

- And any other reasons which we advise you of under a separate policy or notice.

We may also require you to process special categories of information in connection with customers and other third parties.

There may also be circumstances where we ask you to process this type of information in relation to assisting the Company with legal claims or to protect a data subjects interests (or someone else's).
You may be asked to process information in relation to criminal convictions. This should be processed with the highest degree of confidentiality and in accordance with any data protection legislation and privacy notices that are in force in our business.

If you are unsure about how you should process general personal data or special categories of personal data, you must contact Nicki Souter the Company Director or Jayne Mitchell, Data Representative.

When will you need to seek consent?

In limited circumstances during your work you may need consent from a data subject in order to process personal data or special categories of data. You will be provided with training and details of which circumstances consent is needed and the type of consent that should be sought.

However, in limited circumstances, you may find it necessary to request a data subject to provide written consent to allow the processing of special categories of personal data. You will be provided with training and details of which circumstances consent is needed and the type of consent that should be sought. For example, in an employment context you should request the data subject's written consent to instruct a medical practitioner to prepare a medical report. If it becomes necessary to request consent to process special categories of personal data, you must provide the data subject with details of the information that will be required and why it is needed, so that they can make an informed decision as to whether they wish to provide consent.

You must not compel a data subject to provide written consent. Giving consent will always be a decision made by freewill and choice and is not a contractual condition. Consent can be withdrawn at any time without any reason provided. You must not subject a data subject to a sanction or detriment as a consequence of withdrawing consent. This would be viewed a serious disciplinary issue.

Exemptions

In limited circumstance there are certain categories of personal data which are exempt from the GDPR regime. In an employment for example:

- Confidential references that are given, but not those received by the Company from third parties. Only designated line managers can give Company references. Confidential references will not be provided unless the Company is sure this is the employee's wish.
- Management forecasts and management planning (including documents setting out management plans for an employee's future development and progress).
- Data which is required by law to be publicly available.
- Documents subject to legal professional privilege.

Action to be taken in the event of a data protection breach

A personal data breach will arise whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on a data subject.

In the event of a security incident or breach, do not try to handle this yourself.

You must follow the Company's Data Breach Policy which includes immediately informing Nicki Souter the Company Director or Jayne Mitchell, Data Representative so that steps can be taken to:

- Contain the breach;
- Assess the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen; and
- To limit the scope of the breach by taking steps to mitigate the effects of the breach.

Nicki Souter the Company Director or Jayne Mitchell, Data Representative will determine within 72 hours the seriousness of the breach and if the Information Commissioner's Office (ICO) and/or data subjects need to be notified of the breach.

Record keeping

- [As we have fewer than 250 employees, we only need to document processing activities that:
    - are not occasional; or
    - could result in a risk to the rights and freedoms of individuals; or
    - involve the processing of special categories of data or criminal conviction and offence data.]

Training

All employees that handle personal information of individuals must have a basic understanding of the data protection legislation, including the GDPR. Staff with duties such as computer and internet security, marketing and database management may need specialist training to make them aware of particular data protection requirements in their work area.

We will provide you with continuous training and updates on how to process personal data in a secure and confidential manner and in accordance with the spirit of the data protection legislation, including the GDPR. You will be required to attend all training and to keep yourself informed and aware of any changes made to privacy notices, consent procedures and any other policies and procedures associated with our internal processing of personal data.

You must regularly review all your data processing activities and ensure that you are acting in accordance with the most current best practice and legal obligations in relation to data security and confidentiality.

Automated processing and decision making

From time to time we may use computer programmes to process data and make automated decisions. We will provide you with a separate notice explaining when and how this happens. Where automated processing or decision making does take place and the effect of that processing impacts on the freedoms and legitimate interests of the data subject, then in certain circumstances the data subject can request for human intervention. This means that they can ask for a human to review the machine made outcome/decision.

Sharing personal data

We may share personal data internally as is necessary. You must always ensure that personal data is only shared with authorised persons and is shared in accordance with the purposes stated in any privacy notice or consents. Extra care and security must be taken when sharing special categories of data or transferring data outside of the Company to a third party.

Direct Marketing

We are subject to specific rules under the GDPR in relation to marketing our services. Data subjects have the right to reject direct marketing and we must ensure that data subjects are given this option at first point of contact. When a data subject exercises their right to reject marketing you must desist immediately from sending further communications.

Complaints

If you believe that this policy has been breached by a colleague or to exercise all relevant rights, queries or complaints please in the first instance contact Nicki Souter our Company Duirector on 01764 663839

Changes to this policy

We reserve the right to change this policy at any time so please always check this document regularly to ensure you are following the correct procedures.

This policy was last updated on 13th September 2018

Compliance with GDPR is everyone's responsibility.

By signing this policy you confirm that you have read and understood the content of this policy and that you agree to adhere to the content and that you understand that breach of any aspect of this policy may lead to serious disciplinary action.

Signed by name of employee/worker/contractor:

…….

Print name:

……

Date:

…….