Nicholls and Roe Ltd

Data Protection Policy

CONTENTS

Nicholls and Roe Ltd

1. Introduction

The Company needs to gather and use certain information about individuals.

This can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards — and to comply with the law.

2. Why this policy exists

This data protection policy ensures the company;

- complies with data protection law and follows good practice
- protects the rights of all individuals' data
- is open about how it stores and processes individuals' data in line with individuals' rights
- protects itself from the risks of a data breach

3. Data protection law

The General Data Protection Regulations describe how organisations— must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically or otherwise.

To comply with the law, personal information must be;

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Record Keeping:

A range of information must be detailed in our internal records of processing activities. Such areas include;

- name and details of the organisation
- include, if appropriate, details of other data controllers, the organisation's representative and data protection officer
- purposes of processing the data
- description of the categories of individuals and the categories of personal data
- categories of the recipients of personal data
- details of transfers of data to third parties or abroad, including details of safety mechanisms
- retention schedules
- technical and organisational security measures

The company ensures that records of these activities are kept and are updated accordingly. Individuals' data is kept on file for 6 years in line with the Financial Conduct Authorities record keeping rules. After which point, personal data is retracted to the point it is unidentifiable and used for statistical purposes only.

4. Lawful Basis for Processing Data

Under GDPR, it is a requirement that the company has a valid lawful basis to process personal data, this should be documented. Most lawful bases require that processing is 'necessary'.

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever the company process personal data:

Processing is lawful under GDPR as:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

The company has chosen this basis for processing data as it is requested from the individuals that we capture data before entering into a contract (e.g. provide a quote for finance).

Special categories of data may be captured by the company for example, information about an individual's:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;

You need to identify both a lawful basis for general processing and an additional condition for processing this type of data.
If you are processing criminal conviction data or data about offences, you need to identify both a lawful basis for general processing and an additional condition for processing this type of data.

5. Responsibilities

The company acts as a data Controller and data Processor. All staff are responsible for ensuring that the highest data standards and best practices are met on a continual basis.

Although a Data Protection Officer (DPO) has not been appointed as the company does not fall within the scope, the Directors and Owners of the Business are accountable and responsible for compliance with GDPR and will take on the tasks appointed to them as if they were a DPO.

6. Data Protection Impact Assessments (DPIA)

The company has a general obligation to implement technical and organisational measures to demonstrate that data protection is integrated into our processing activities. A Data Protection Impact Assessment is conducted each time the company consider implementing using new technologies

The DPIA will pertain at least;

- a description of the processing operations and the purposes, including, where applicable, the legitimate interests pursued by the controller;
- an assessment of the necessity and proportionality of the processing in relation to the purpose;
- an assessment of the risks to individuals;
- the measures in place to address risk, including security and to demonstrate that you comply.

7. Individuals Rights

Individuals now have more rights under GDPR, the company, these are;

- the Right to be Informed
- the Right of Access
- the Right to Rectification
- the Right to Erasure
- the Right to Restrict Processing
- the Right to Data Portability
- the Right to Object
- rights in relation to automated decision making and profiling.

The company provide every customer with a Privacy Notice at the point data is captured.

The information supplied in this notice demonstrates how the company is transparent over our data processing. The notice is;

- concise, transparent, intelligible and easily accessible;
- written in clear and plain language, particularly if addressed to a child; and free of charge.

We include details of (but not limited to);

the Data Controller, the lawful reason for processing data, if any third parties have legitimate interests, categories of personal data, categories of recipients such as banks and credit unions, the data retention periods,

the individuals' rights; including the right to withdraw, where the individual can complain about how the data is processed with a supervisory authority, source of data when it comes from a third party and where personal data is part of a contractual requirement or obligation.

Rectification

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete. If the company has disclosed the personal data in question to third parties, then we will inform them of the rectification where possible.

The company will respond to this request within one month or extended by two months where the request for rectification is complex.

Erasure

Individuals have a right to have personal data erased and to prevent processing in specific circumstances;

- where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.

- when the individual withdraws consent.
- when the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- the personal data was unlawfully processed (i.e. otherwise in breach of the GDPR).
- the personal data must be erased to comply with a legal obligation.
- the personal data is processed in relation to the offer of information society services to a child.
- under the GDPR, this right is not limited to processing that causes unwarranted and substantial damage or distress. However, if the processing does cause damage or distress, this is likely to make the case for erasure stronger.

The company may refuse to comply with a request for erasure where the personal data is processed for the following reasons;

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation for the performance of a public interest task or exercise of official authority.
- for public health purposes in the public interest;
- archiving purposes in the public interest, scientific research historical research or statistical purposes; or
- the exercise or defence of legal claims.

If the company has disclosed the personal data in question to third parties, a notification will be sent, informing them about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

Restrict processing

The company will restrict the processing of personal data in the following circumstances;

- where an individual contest the accuracy of the personal data, you should restrict the processing until you have verified the accuracy of the personal data.
- where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and you are considering whether your organisation's legitimate grounds override those of the individual.
- when processing is unlawful, and the individual opposes erasure and requests restriction instead.
- if you no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.

if any data has been disclosed to third parties, the company will notify them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

Portability

For personal data an individual has provided to a controller; where the processing is based on the individual's consent or for the performance of a contract; and when processing is carried out by automated means, the company must provide the personal data in a structured, commonly used and machine-readable form. Open formats include CSV files. Machine readable means that the information is structured so that software can extract specific elements of the data. This enables other organisations to use the data.

The company must provide this service free of charge.

If the individual requests it, we may be required to transmit the data directly to another organisation if this is technically feasible. The company will respond without undue delay, and within one month or extended by two months where the request is complex or receive many requests.

Objecting

If an individual has objected to processing data or direct marketing, the company will cease to process the data.

Individuals must have an objection on "grounds relating to his or her particular situation".

The company will stop processing the personal data unless**;**

- compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
- the processing is for the establishment, exercise or defence of legal claims.

This is brought to the attention of the data subject at the first point of communication and in our privacy notice. This is separated out from any other information.

Direct marketing purposes

As soon as an objection is received, the company will stop processing personal data for direct marketing purposes. This will be actioned at any stage and is free of charge.

Automated decision making including profiling

The company understand that any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse, or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour falls under this right. Where this is conducted, the rules and guidance of the ICO will be adhered to and followed. To date, the company does not conduct automated decision-making including profiling.

8. Subject Access Requests (SAR)

Individuals who are the subject of personal data held by the company are entitled to;

- confirmation that their data is being processed;
- access to their personal data; and

- other supplementary information – this largely corresponds to the information that should be provided in a privacy notice

Individuals contacting the company requesting this information, this is called a Subject Access Request.

The company will provide a copy of the information free of charge. However, a 'reasonable fee' may be charged when a request is manifestly unfounded or excessive, particularly if it is repetitive.

A reasonable fee may also be charged to comply with requests for further copies of the same information. The fee is based on the administrative cost of providing the information only.

Once the identity of the person making the request has been verified, the information will be provided within 1 month, this will be extended to 2 months if the request is complex. Notification will be made to the individual if this is the case.

9. Complaints

It is made clear that data subjects who wish to complain about how their personal data has been processed can raise this with the company complaints procedure. If the data subject is still not happy, then the complaint can be referred to the Information Commissioners Office.

10. Data Security and Storage

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see or have access to it. These guidelines also apply to data that is usually stored electronically but has been printed out for some reason;

- when not required, the paper or files should be kept in a locked drawer or filing cabinet.
- employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer;
- data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts;

- data should be protected by strong passwords or encryption products;
- if data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used;
- data should only be stored on designated drives and servers and should only be uploaded to an approved cloud computing services;
- servers containing personal data should be sited in a secure location, away from general office space;
- data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures;
- data should never be saved directly to laptops or other mobile devices like tablets or smart phones;
- all servers and computers containing data should be protected by approved security software and a firewall.

The point that personal data is accessed is when it can be at greatest risk of loss, corruption, theft, unlawful access, the company will;

- when working with personal data, employees should ensure the screens of their computers are always locked when left unattended;
- personal data should not be shared informally. It should never be sent by email, as this form of communication is not secure.
- data must be encrypted before being transferred electronically.
- personal data should never be transferred outside of the European Economic Area unless contractual arrangements are in place highlighting adequate safeguards and protection to the rights of individuals.
- employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.