NORSE CONTRACTING LIMITED

DATA PROTECTION POLICIES

Contents

Data Protection Policy (compliant with GDPR)

Purpose

As a Company we are committed to being transparent about how we collect and use your personal data. This sets out our commitment to data protection, and individual rights and obligations in relation to personal data.

This policy applies to the personal data of job applicants, employee's, workers, contractors, volunteers, interns, apprentices and former employees, referred to as HR-related personal data. As well as our clients and customers

Definitions

- **"Personal data"** is any information that relates to an individual who can be identified from that information. Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

- **"Special categories of personal data"** information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

- **"Criminal records data"** information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

- **"Data Subject"** an individual who is the subject of personal data

Data protection principles

- We process personal data in accordance with the following data protection principles:

  - We process personal data lawfully, fairly and in a transparent manner.
  - We collect personal data only for specified, explicit and legitimate purposes.
  - We process personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
  - We keep accurate personal data and take all reasonable steps to ensure that any inaccurate personal data is rectified or deleted without delay.
  - We keep personal data only for the period necessary for processing.
  - We adopt appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

- We will tell individuals the reasons for processing their personal data, how we use such data and the legal basis for processing our privacy notices. We will not process personal data of individuals for other reasons.

- We will update your HR-related personal data promptly upon you advising us that your information has changed or is inaccurate.

- All information we hold on you is held on your personnel file (in hard copy or electronic format, or both). The periods for which the organisation holds HR-related personal data are contained in its privacy notices to individuals and in document control.

Individual rights

You have a number of rights in relation to your personal data.

Subject access requests

You have the right to make a subject access request. After making a request, we will let you know, one of the following:

- Whether or not your data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;
- To whom your data is or may be disclosed;
- For how long your personal data is stored (or how that period is decided);
- Your rights to rectification or erasure of data, or to restrict or object to processing;
- Your right to complain to the Information Commissioner if you think we have failed to comply with your data protection rights; and

Subject Access Request Process

- You should send an email request to the Operations Director, for ex-employees we may ask for proof of identification.
- We will normally respond to a request within a period of one month from the date it is received. However, if we process a large amount of the individual's data, we reserve the right to extend this timescale.
- Where subject access request is obviously unfounded or excessive, we are not obliged to comply with it. Or, we can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request.
- If we have already responded to subject access request and you re submit this request, it is likely to be unfounded or seen as excessive.
- If an individual submits a request that is unfounded or excessive, we will notify them that this is the case and whether or not we will respond to it.

Other rights

You have a number of other rights in relation to your personal data. You have the right to:

- Rectify inaccurate data;
- Stop processing or erase data that is no longer necessary for the purposes of processing;
- Stop processing or erase data if your interests override the Company's legitimate grounds for processing data (where we rely on its legitimate interests as a reason for processing data);
- Stop processing or erase data if processing is unlawful; and
- Stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override the Company's legitimate grounds for processing data.

Data security

We take the security of HR-related personal data seriously. We have internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

- We have the following policies in place to protect personal data:
  - Bring your own device to work policy
  - Communication, email, internet & social media policy which includes security & security breaches
  - Data Retention policy
- Where we engage third parties to process personal data on our behalf, we put measures in place to ensure they are compliant with GDPR.

Data breaches

- We encourage anyone who breaches any HR-related personal data to report it immediately, regardless of how minor it may seem, all minor data breaches must be reported and logged. However, breach of personal data that poses a risk to the rights and freedoms of individuals, it will be reported to the Information Commissioner within 72 hours of discovery.
- If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

International data transfers

We will not transfer HR-related personal data to countries outside the EEA.

Your responsibilities

- You are responsible for helping the Company keep your personal data up to date. You should let us know if data provided to us changes, for example if you move house or change your bank details.

- You may have access to the personal data of other individuals and of our customers and clients in the course of your employment. Where this is the case, we rely on you to help meet our data protection obligations to staff and to customers and clients.

- Individuals who have access to personal data are required:

    - to access only data that they have authority to access and only for authorised purposes;
    - not to disclose data except to individuals (whether inside or outside the Company) who have appropriate authorisation;
    - to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
    - not to remove personal data, or devices containing or that can be used to access personal data, from the organisation's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and
    - not to store personal data on local drives or on personal devices that are used for work purposes.

- Further details about the organisation's security procedures can be found in:
    - Bring your own device to work policy
    - Communication, email, internet & social media policy which includes security & security breaches
    - Data Retention policy

- Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

Training

- We will provide training to you about your data protection responsibilities.

- If you have a role which requires regular access to personal data, or if you are responsible for implementing this policy or responding to subject access requests under this policy, you will receive additional training to help them understand their duties and how to comply with them.

Data Retention Policy

We have obligations regarding retention of personal data collected, held, and processed by the Company in accordance with EU Regulation 2016/679 General Data Protection Regulation ("GDPR").

- Under the GDPR, personal data shall be kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.

- In addition, the GDPR includes the right to erasure or "the right to be forgotten". Data subjects have the right to have their personal data erased (and to prevent the processing of that personal data) in the following circumstances:

    - Where the personal data is no longer required for the purpose for which it was originally collected or processed;
    - When the data subject withdraws their consent;
    - When the data subject objects to the processing of their personal data and the Company has no overriding legitimate interest;
    - When the personal data is processed unlawfully (i.e. in breach of the GDPR);
    - When the personal data has to be erased to comply with a legal obligation;

- This Policy sets out the type(s) of personal data held by the Company for contract, legal & legitimate purposes, the period(s) for which that personal data is to be retained, the criteria for establishing and reviewing such period(s), and when and how it is to be deleted or otherwise disposed of.

- For further information on other aspects of data protection and compliance with the GDPR, please refer to the **Data Protection policy**.

Aims and objectives

- The primary aim of this policy is to set out limits for the retention of personal data and to ensure that those limits, as well as further data subject rights to erasure, are complied with. By extension, this Policy aims to ensure that the Company complies fully with its obligations and the rights of data subjects under the GDPR.

- In addition to safeguarding the rights of data subjects under the GDPR, by ensuring that excessive amounts of data are not retained by the Company, this policy also aims to improve the speed and efficiency of managing data.

Scope

- This policy applies to all personal data held by us and by third-party data processors who process personal data on the Company's behalf.

- Personal data, as held by the Company & third parties is stored in the following ways and in the following locations:
    - Computers permanently located in the Company's premises at **54a Ashburnham**

Road, Northampton NN1 4QY;

- Laptop computers and other mobile devices provided by the Company to its employees;
- Physical records stored at **Hallet & Associates (Accountants)**

Data subject rights and data integrity

- Any personal data we hold in accordance with the requirements of the GDPR and data subjects' rights, as set out in the Company's **Data Protection policy** is:

  - We keep data subjects fully informed of their rights, regarding what we hold on them and how we use it. As well as how long the data is stored for (or, if no fixed retention period can be determined, the criteria by which the retention of the data will be determined).
  - We give data subjects control over the personal data held by us, including the right to have incorrect data rectified, the right to request that their personal data be deleted or otherwise disposed of (notwithstanding the retention periods otherwise set by this Data Retention policy), the right to restrict the Company's use of their personal data as set out in **Data Protection policy**.

Organisational Data Security Measures

- We have measures in place to ensure the security of all of our personal data:

  - Everyone who works for us shall be made fully aware of both their individual responsibilities and our responsibilities under the GDPR;
  - Only employees and other parties working on behalf of the Company that need access to, and use of, personal data in order to perform their work shall have access to the personal data;
  - All employees and other parties working on behalf of the Company handling personal data will be appropriately trained to do so;
  - All employees and other parties working on behalf of the Company handling personal data should exercise care and caution when discussing any work relating to personal data at all times;
  - We will evaluate and review methods of collecting, holding, and processing personal data;
  - If you are required as part of your role to handle personal data, you will be bound by the contract to comply with the GDPR and the Company's Data Protection Policy;
  - Where any agent, contractor or other party working on behalf of the Company handling personal data fails in their obligations under the GDPR and/or the Company's Data Protection Policy, that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

Data disposal

- We will ensure we comply with data retention periods when data gets expired, or when a data subject exercises their right to have their personal data erased, personal data shall be deleted, destroyed, or otherwise disposed of as follows:

- Personal data stored electronically (including any and all backups thereof) shall be deleted securely;
- Special category personal data stored electronically (including any and all backups thereof) shall be deleted securely;
- Personal data / special category data stored in hardcopy form must be shredded using at least a Level 3 category shredder and recycled;

Data retention

- As stated above, and as required by law, we shall not retain any personal data for any longer than is necessary in light of the purpose(s) for which that data is collected, held, and processed.

- Different types of personal data, used for different purposes, will be retained for different periods (in line with legislation), and its retention periodically reviewed, as set out below.

- When establishing and/or reviewing retention periods, the following shall be taken into account:
  - Our objectives and requirements;
  - The type of personal data in question;
  - The purpose(s) for which the data in question is collected, held, and processed;
  - The legal basis for collecting, holding, and processing that data;
  - The category or categories of data subject to whom the data relates;

- If a precise retention period cannot be fixed for a particular type of data, we will regularly review the reasons for retention.

- Notwithstanding the following defined retention periods, certain personal data may be deleted or otherwise disposed of prior to the expiry of its defined retention period where a decision is made within the Company to do so (whether in response to a request by a data subject or otherwise).

Roles and responsibilities

- The **Senior Recruitment Consultant** shall be responsible for overseeing the implementation of this Policy and for monitoring compliance.

- All Managers shall be directly responsible for ensuring compliance with the above data retention periods throughout the Company.

- Any questions regarding this Policy, the retention of personal data, or any other aspect of GDPR compliance should be referred to your line manager.

Communications, Email, Internet & Social Media policy

Our Communications, Email, Internet & Social Media Policy applies to all employees, contractors and agents of the Company who use the communications equipment and systems.

Any communication you make whether it be by email or telephone reflects upon the Company. So, we have created this policy to clarify what we expect from you and your responsibility when using the Company's communications facilities.

- "Communications equipment & systems could include:

    - Telephone
    - Email
    - Internet
    - And any other communication device or network provided.

General Principles

- We would like you to be mindful of the following when communicating either externally or internally:

    - Use communications equipment and facilities responsibly and professionally
    - Be mindful of what constitutes confidential or restricted information and to ensure that such information is never disseminated in the course of communications without express authority
    - Ensure that you do not breach any copyright or other intellectual property right when making communications
    - Ensure that you do not bind yourself or the Company to any agreement without express authority to do so
    - Be mindful of the fact that any communication may be required to be relied upon in court, to the advantage or the detriment of the individual or the Company and conduct your use of communication systems and equipment accordingly.

Internet

- We provide access to the internet for the sole purpose of business and to assist you in your duties. However, we do allow use of the internet for personal purposes as long as is outside of the working hours, such as in your lunch break.

- You may be asked to justify the amount of time you have spent on the internet or the sites you have visited.

- We state you must not:

    - Use the internet to gain or attempt to gain unauthorised access to computer material, including restricted areas or confidential information of the Company's network.
    - Download or install any software without the express permission of a Director. Nor must you intentionally or recklessly introduce any form of malware, spyware, virus or other malicious software or code to or using the communications equipment or systems of the Company.

- Attempt to download, view or otherwise retrieve illegal, pornographic, sexist, racist, and offensive or any other material which may cause embarrassment to the corporate image of the Company.
- Do not enter in to any contracts or commitments in the name of or on behalf of the Company.

- Any such attempt will constitute a disciplinary offence and in addition to internet access being reviewed, reduced or withdrawn, may be subject to disciplinary action or summary dismissal.

Removing internet access

We reserve the right to deny access to any employee at work, although in such a case it will endeavour it to give reasons for doing so.

When and how the internet will be monitored:

- We reserve the right to monitor your internet usage but will inform you if we need to and our reason for doing so. However, we will check usage for the following reasons:

  - Viewing offensive or illegal material, such as material containing racist terminology or nudity (although we understand that it is possible to inadvertently view such material and they will have the opportunity to explain if this is the case).
  - If we suspect you have been spending excessive amounts of time visiting websites that are not work related.

- Monitoring will consist of checking the websites visited and the duration of such visits.

Data protection

- We carry out monitoring as it the Company's legitimate interests and to ensure the policy is being complied with.

- The Senior Recruitment Consultant will be responsible for carrying out any monitoring and the findings will only be shared where there is a need to investigate such as a breach of the rules. We will only share it with third party of we have a duty to report matter such as to a regulatory authority

- You have a number of rights in relation to your data, including the right to make a subject access request and the right to have data rectified or erased in some circumstances.

Use of Company Email

- We will provide you with a Company email address, to be used for all business purposes; you should never use your personal email when communicating on Company business.

- We recognise that there may be instances where you may need to use your Company email address for personal reasons. This is permitted on the condition that such use is kept to a minimum and does not interfere with the performance of your duties. Personal emails from your Company email may be subject to monitoring.

- You should at all times remember that email messages may have to be disclosed as evidence for any court proceedings or investigations by regulatory bodies and may therefore be prejudicial to both their and the Company's interests. This includes data which appears to have been deleted as it is often recoverable.

Contents of Email

- We request that you check your emails to make sure that it makes sense and there are no spelling mistakes. Any emails sent that are defamatory, obscene or otherwise inappropriate will be treated as misconduct or gross misconduct.

- You must be sure that the email is addressed to the correct person especially when sending client personal information as this could result in a data breach.

- Equally, if you receive an obscene or defamatory email, whether unwittingly or otherwise and from whatever source, you should not forward it to any other address.

- You should not send an email that will bring the Company in to disrepute, this includes criticising competitors.

Attachments

- You should not attach any files that may contain a virus to emails, as the Company could be liable to the recipient. We do have virus-checking in place but, if in doubt, check first.

- We ask that you should exercise extreme care when receiving emails with attachments from third parties, particularly unidentified third parties, as these may contain viruses.

Personal Email

- You are permitted to access and use your personal email accounts only to when it is outside of work time, for instance in your lunch break.

When & how email will be monitored

We consider the following to be valid reasons for checking an employee's email:

- Absent for any reason and emails must be checked for the smooth running of the business.

- If we suspect offensive or illegal material, such as material containing racist terminology or nudity has been viewed.

- If we suspect the Company email has been used to send and receive an excessive number of personal communications.

- If we suspect Company emails are being sent or received are detrimental to the Company.

When monitoring emails, we will, endeavour to, just look at the address and subject heading of the emails. Where possible, we will avoid opening emails clearly marked as private or personal.

However, we would encourage you not to send & receive sensitive and confidential communications because it cannot be guaranteed to be private.

Social media

This section outlines what is acceptable regarding of all types of social network and social media platforms including, but not limited to, Facebook, Twitter, LinkedIn, Google+, Pinterest, Tumblr, Instagram, Snapchat (collectively, "Social Media"). Social media also covers blogs and video and image-sharing websites such as YouTube.

There are many more examples of social media that are not listed here as this is a constantly changing area. You should follow these guidelines in relation to any social media that you use.

Limited use of social media

- You may use Social Media for personal purposes occasionally during work hours for example, during breaks providing you comply with this Policy.

Use of social media at work

- We may ask you to use social media to promote something for the Company. As part of your role you may be required to use social media to promote the Company. This could be contributing to our blogs / a Facebook post.

- Company email addresses may only be used to sign up to Social Media websites for work-related purposes.

- You must be aware at all times that, when putting anything on the Company's social media, you are representing the Company. You must ensure you have,

    - obtained permission from a manager before starting on a public campaign using social media; and
    - get a colleague to check the content before it is published.

- You must not:

    - bring the Company into disrepute, for example by:
        - criticising or arguing with customers, colleagues or rivals;
        - making defamatory comments about individuals or other companies or groups; or
        - posting images that are inappropriate or links to inappropriate content;

    - breach confidentiality, for example by:
        - revealing any trade secrets;
        - giving away confidential information about an individual (such as a colleague or customer contact) or company (such as a rival business); or
        - discussing the Company or its future business plans that have not been made public);

- breach copyright, for example by:
    - using someone else's images or written content without permission;
    - failing to give acknowledgement where permission has been given to reproduce something; or

- do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
    - making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
    - using social media to bully another individual; or
    - posting images that are discriminatory or offensive or links to such content.

Monitoring use of social media during work time

- We reserve the right to monitor employees' use of social media on the Company's equipment for what we consider are valid reasons, such as:

    - been using social media when they should be working; or
    - acted in a way that is in breach of the rules set out in this policy.

- Monitoring is in our legitimate interests and to ensure that this policy on use of social media is being complied with.

- We will check the social media sites visited and the duration of such visits and the content contributed on such sites.

- A Director will be responsible for carrying out any monitoring and the findings will only be shared where there is a need to investigate such as a breach of the rules. We will only share it with third party of we have a duty to report matter such as to a regulatory authority

- Access to particular social media may be withdrawn in cases of misuse.

Social media outside of work

- We know that most of you will use social media personally outside of work. However, you must be aware that you can damage the Company if you are recognised as being one of our employees.

- We would never stop you from saying where you work, and we recognise that it is natural for you to sometimes want to discuss your work on social media. However, we would not expect you to post defamatory comments about the Company.

Disciplinary action over social media use

All employees are required to adhere to this policy. Employees should note that any breaches of this policy may lead to disciplinary action. Serious breaches of this policy, for example incidents of bullying of colleagues or social media activity causing serious damage to the organisation, may constitute gross misconduct and lead to summary dismissal.

Security

- The integrity of our business relies on the security of its communications equipment and systems. You bear the responsibility of preserving the security of communications equipment and systems through careful and cautious use.

- You should adopt the following points as part of best practice:

  - You must not share any password that you use for accessing Company communications equipment and systems with any person, other than when it is necessary for maintenance or repairs. Where it has been necessary to share a password, you should change the password immediately. You are reminded that it is good practice to change passwords regularly.
  - You must ensure that confidential and sensitive information is kept secure.
  - iPads should be locked when you are not using it, hard copy files and documents should be secured when not in use and caution should be exercised when using mobile telephones outside of the workplace.
  - When opening email from external sources you must exercise caution in light of the risk of viruses. You should always ensure that you know what an attachment is before opening it. If you suspect that your computer has been affected by a virus you must contact your line manager immediately.
  - No external equipment or device may be connected to or used in conjunction with the Company's equipment or systems without the prior express permission of your line manager.

Reporting IT security breaches

- All concerns, questions, suspected breaches or known breaches shall be referred immediately to the **Senior Recruitment Consultant**.

- Upon receiving a question or notification of a breach, we shall, assess the issue and take any steps deemed necessary to respond to the issue.

- Under no circumstances should you attempt to resolve an IT security breach on your own without first consulting the **Senior Recruitment Consultant**. You may only attempt to resolve IT security breaches under the instruction of, and with the express permission of, the **Senior Recruitment Consultant**.

- All IT security breaches, regardless of severity shall be fully documented.

Company IT property

- If you are supplied with a laptop or other, IT hardware as part of your role then it is on the understanding that this is to enable you to carry out your role and therefore there should be only very limited personal use.

- Any use is covered by the guidelines outlined in the sections above, even if out of working hours.

Bring your own device (BYOD) to work policy

This policy applies to all employees who use their personal computers and/or other electronic devices, such as smartphones for work. We have put this policy in place to protect the security and integrity of any personal data we may hold and in line with GDPR. It should be read in conjunction with the Company's **Communications, Email, Internet and Social Media Policy**.

The policy also covers those employees who occasionally receive work-related emails on their mobile telephones.

As long as you have prior permission then you are permitted to use your own devices for work-related purposes.

Special category data

You are not permitted to process or hold special category data on a personal device, "special category data" is information about an individual's:

- racial or ethnic origin;
- political opinions;
- religious beliefs or philosophical beliefs;
- trade union membership (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992);
- physical or mental health or condition (including genetic or biometric data); and sex life or sexual orientation.

- Information related to criminal records and convictions is also treated as special category data for the purposes of this policy.

Your obligations regarding BYOD

Security

- When using your own device for work you must ensure that you use a strong password to lock the device. The device must be capable of locking automatically if an incorrect password is entered after several attempts or if the device is inactive.

- In addition, you must:

  - use encryption software on your devices to store personal data securely;
  - ensure that if you transfer Company data (either by email or by other means), you do so via an encrypted channel (for example a VPN for individual services);
  - ensure that you assess the security of any open network or Wi-Fi connection (employees should not use unsecured Wi-Fi networks);
  - not, under any circumstances, use Company personal information for any purpose other than for your work;
  - use different applications for business and personal use;

- ensure that you have a system of software in place for quickly and effectively revoking access that a user might gain to a device in the event of loss or theft;
- report the loss or theft of a device used for work-related activities immediately to a member of the Operations Director and
- report data breaches as soon as become aware to the Operations Director.

- You must not use public cloud-based sharing or public back-up services.

- If you sell or give away your device, you will need to ensure all Company data is deleted.

Mobile-device management

- To safeguard Company information in the event that your device is stolen, you should be able to access the device remotely to ensure you can delete any Company date contained on it.

Retention of personal data

- Personal data shouldn't be retained for longer than is necessary, unless there is a requirement to retain it for longer to comply with any legal obligation.

Deletion of personal data

- Deleted information should be deleted permanently rather than left in the device's waste-management system. We do not expect you to have overwriting software, in this case you must:

  - not give any other Company access to the personal data in any way;
  - make sure the personal data is secure; and
  - commit to the permanent deletion of the information if and when this becomes possible.
  - If you use removable media, for example a USB stick, to transfer personal data, you must ensure that the personal data is deleted once the transfer is complete.

Co-operation with subject access requests

- Under the Data Protection Regs (GDPR) any individual (this could be a customer or employee) whose personal data is held by any Company has the right to make a subject access request (see the **Data Protection policy**). If a subject access request is made, we may need to access your device to retrieve any data that is held on it about the individual. You must allow the Company to access the device and to carry out a search to find any information about the individual held on the device.

Third-party use of device

- If you allow family or friends use your device, they must not be able to gain access to any work related information, for example, password-protecting it.

Termination of employment

- If you leave the Company, you must delete all work-related personal data on your own device prior to your last day with the Company.

Monitoring

- As part of our obligations under the GDPR, we will monitor data protection compliance in general and compliance with this policy. Monitoring is in our legitimate interests and to ensure that this policy is being complied with.

- The Senior Recruitment Consultant will be responsible for carrying out any monitoring and the findings will only be shared where there is a need to investigate such as a breach of the rules. We will only share it with third party of we have a duty to report matter such as to a regulatory authority.

- Information obtained through monitoring will not be disclosed to third parties (unless the Company is under a duty to report matters to a regulatory authority or to a law enforcement agency.

Consequences of non-compliance

- Anyone suspected of breaching this policy, will be subject to a disciplinary procedure. If any breaches are established, this could result in disciplinary action up to and including dismissal. An employee may also incur personal criminal liability for breaching this policy.

Review of procedures and training

- We will provide training to employees on data protection matters on induction and on a regular basis thereafter. If you consider that you will benefit from refresher training, you should contact your line manager.