TRP Data Protection Policy.

(TRP Data Protection policy 10.05.18)

Updated 16.11.18

Data Protection Policy.

1 Overview

1.1 The Company takes the security and privacy of your data seriously. We need to gather and use information or 'data' about you as part of our business and to manage our relationship with you. We intend to comply with our legal obligations under the Data Protection Act 2018 (the '2018 Act') and the EU General Data Protection Regulation ('GDPR') in respect of data privacy and security. We have a duty to notify you of the information contained in this policy.

1.2 This policy applies to current and former employees, TRP's supplier and customer contacts and other third parties with which it is in contact. If you fall into one of these categories then you are a 'data subject' for the purposes of this policy. You should read this policy alongside your contract of employment (or contract for services) and any other notice we issue to you from time to time in relation to your data.

1.3 The Company has measures in place to protect the security of your data in accordance with our policy.

1.4 The company will hold data in accordance with our policy. We will only hold data for as long as necessary for the purposes for which we collected it.

1.5 The Company is a **'data controller'** for the purposes of your personal data. This means that we determine the purpose and means of the processing of your personal data.

1.6 This policy explains how the Company will hold and process your information. It explains your rights as a data subject. It also explains your obligations when obtaining, handling, processing or storing personal data in the course of working for, or on behalf of, the Company.

1.7 This policy does not form part of your contract of employment (or contract for services if relevant) and can be amended by the Company at any time. It is intended that this policy is fully compliant with the 2018 Act and the GDPR. If any conflict arises between those laws and this policy, the Company intends to comply with the 2018 Act and the GDPR.

2 Data Protection Principles

2.1.1 Personal data must be processed in accordance with six '**Data Protections Principles'**. It must:

- Be processed fairly, lawfully and transparently;
- Be collected and processed only for specified, explicit and legitimate purposes;

- Be adequate, relevant and limited to what is necessary for the purposes for which it is processed;
- Be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay;
- Not be kept for longer that is necessary for the purposes for which it is processed; and
- Be processed securely.

We are accountable for these principles and must be able to show that we are compliant.

3 How we define personal data

3.1 '**Personal data'** means information which relates to a living person who can be **identified** from that data (a '**data subject'**) on its own, or when taken together with other information which is likely to come into our possession. It includes any expression of opinion about the person and an indication of the intentions of us or others, in respect of that person. It does not include anonymised data.

3.2 This policy applies to all personal data whether it is stored electronically, on paper or on other materials.

3.3 This personal data might be provided to us, by you, or someone else (such as a former employer, your doctor, or a credit reference agency), or it could be created by us. It could be provided or created during the recruitment process or during the course of the contract of employment (or services) or after its termination. It could be created by your manager or other colleagues.

3.4 We will collect and use the following types of personal data about you:

- Recruitment information such as your application form and CV, references, qualifications and membership of any professional bodies and details of any pre-employment assessments;
- Your contact details including your email address and date of birth;
- The contact details for your emergency contacts;
- Your gender;
- Information about your contract of employment (or services) including start and end dates of employment, role and location, working hours, details of promotion, salary (including details of previous remuneration), pension, benefits and holiday entitlement;
- Your bank details and information in relation to your tax status including your national insurance number;
- Your identification including passport and driving licence and information in relation to your immigration status and rights to work for us;
- Information relating to your performance and behaviour at work;
- Training records;
- Electronic information in relation to your use of IT systems/swipe cards/clocking cards/ telephone systems;

- Your images (whether captured on CCTV, by photograph or video); and
- Any other category of personal data which we may notify you of from time to time.

4 How we define special categories of personal data

4.1 'Special categories of personal data' are types of personal data consisting of information as to:

- Your racial or ethnic origin;
- Your political opinions;
- Your religious or philosophical beliefs;
- Your trade union membership;
- Your genetic or biometric data;
- Your health;
- Your sex life and sexual orientation; and
- Any criminal convictions and offences.

We may hold and use any of these special categories of your personal data in accordance with the law.

5 How we define processing

5.1 means any operation which is performed on personal data such as:

- Collection, recording, organisation, structuring or storage;
- Adaption or alteration;
- Retrieval, consultation or use;
- Disclosure by transmission, dissemination or otherwise making available;
- Alignment or combination; and
- Restriction, destruction or erasure.

This includes processing personal data which forms part of a filing systems and any automated processing.

6 How will we process your personal data?

6.1 The Company will process your personal data (including special categories of personal data) in accordance with our obligations under the 2018 Act.

6.2 We will use your personal data for:

- Performing the contract of employment (or services) between us;
- Complying with any legal obligation; or
- If it is necessary for our legitimate interests (or for the legitimate interests of someone else). However, we can only do this if your interests and rights do not override ours (or theirs). You have the rights to challenge our legitimate interests and requests that we stop this processing. See details of your rights in section 12 below.

We can process your personal data for these purposes without your knowledge or consent. We will not use your personal data for an unrelated purpose without telling you about it and the legal basis that we intend to rely on for processing it.

If you choose not to provide us with certain personal data you should be aware that we may not be able to carry out certain parts of the contract between us. For example, if you do not provide us with your bank account details we may not be able to pay you. It might also stop us from complying with certain legal obligations and duties which we have such as to pay the right amount of tax to HMRC or to make reasonable adjustments in relation to any disability you may suffer from.

7.1 **Examples of when TRP might process your personal data as an employer or as a Company you are engaged with.**

7.1.1 We have to process your personal data in various situations during your recruitment, employment (or engagement) and even following termination of your employment (or engagement).

7.1.2 For example (and see section 7.1.5 below for the meaning of the asterisks):

- To decide whether to employ (or engage) you;
- To decide how much to pay you, and the other terms of your contract with us;
- To check you have the legal right to work for us;
- To carry out the contract between us including where relevant, its termination;
- Training and reviewing your performance*
- To decide whether to promote you ;
- To decide whether and how to manage your performance, absence or conduct*
- To carry out a disciplinary or grievance investigation or procedure in relation to you or someone else ;
- To determine whether we need to make reasonable adjustments to your workplace or role because of your disability*
- To monitor diversity and equal opportunities*
- To monitor and protect the security (including network security) of the Company, of you, our other staff, customers and others ;
- To monitor and protect the health and safety of you, our other staff, customers and third parties*
- To pay you and provide pension and other benefits in accordance with the contract between us*
- Paying tax and national insurance;
- To provide a reference upon request from another employer;
- To pay trade union subscriptions*
- Monitoring compliance by you, us and others with our policies and out contractual obligations*
- To comply with employment law, immigration law, health and safety law, tax law and others laws which affect us*
- To answer questions from insurers in respect of any insurance policies which relate to you*
- Running our business and planning for the future;

- The prevention and detection of fraud or other criminal offences;
- To defend the Company in respect of any investigation or litigation and to comply with any court or tribunal orders for disclosure*
- For any other reason which we may notify you of from time to time.

7.1.3 We will only process special categories of your personal data (see above) in certain situations in accordance with the law. For example, we can do so if we have your explicit consent. If we asked for your consent to process a special category of personal data then we would explain the reasons for our request. You do not need to consent and can withdraw consent later if you choose by contacting Mariana Dumitru by email at mariana.dumitru@trpsealing.com.

7.1.4 We do not need your consent to process special categories of your personal data when we are processing it for the following purposes, which we may do:

- Where it is necessary for carrying out rights and obligations under employment law;
- Where it is necessary to protect your vital interests or those of another person where you/they are physically or legally incapable of giving consent;
- Where you have made the data public;
- Where processing is necessary for the establishment, exercise or defence of legal claims; and
- Where processing is necessary for the purposes of occupational medicine or for the assessment of your working capacity;

7.1.5 We might process special categories of your personal data for the purposes in paragraph 7.2 above which have an asterisk beside them. In particular, we will use information in relation to:

- Your race, ethnic origin, religion, sexual orientation or gender to monitor equal opportunities;
- Your sickness absence, health and medical conditions to monitor your absence, assess your fitness for work, to pay you benefits, to comply with our legal obligations under employment law including to make reasonable adjustments and to look after your health and safety; and
- Your trade union membership to pay any subscriptions and to comply with our legal obligations in respect of trade union members.

7.1.6 We do not take automated decisions about you using your personal data or use profiling in relation to you.

7.2 Example of when TRP might process your personal data as a Company you have business dealings.

Your business email address is regarded as personal data as such the Company will ask you to positively consent to the Company holding your email address.

8 Sharing your personal data

Sometimes we might share your personal data with group companies or our contractors and agents to carry out our obligations under our contract with you or for our legitimate interests.

We require those companies to keep your personal data confidential and secure and to protect it in accordance with the law and our policies. They are only permitted to process your data for the lawful purpose for which it has been shared and in accordance with our instructions.

We do not send your personal data outside the European Economic Area. If this changes you will be notified of this and the protections which are in place to protect the security of your data will be explained.

How should you process personal data for the Company?

8.1 Everyone who works for, or on behalf of, the Company has some responsibility for ensuring data is collected, stored and handled appropriately, in line with this policy and the Company's data security and data retention policies.

8.2 The Company's Data Protection Manager is Mariana Dumitru (email address: mariana.dumitru@trpsealing.com) who is responsible for reviewing this policy and updating the Board of Directors of the Company's data protection responsibilities and any risks in relation to the processing of data. You should direct any questions in relation to this policy or data protection to this person.

8.3 You should only access personal data covered by this policy if you need it for the work you do for, or on behalf of the Company and only if you are authorised to do so. You should only use the data for the specified lawful purpose for which it was obtained.

8.4 You should not share personal data informally.

8.5 You should keep personal data secure and not share it with unauthorised people.

8.6 You should regularly review and update personal data which you have to deal with for work. This includes telling us if your own contact details change.

8.7 You should not make unnecessary copies of personal data and should keep and dispose of any copies securely.

8.8 You should use strong passwords.

8.9 You should lock your computer screens when not at your desk.

8.10 Personal data shall as far as possible be encrypted before being transferred electronically to authorised external contacts.

8.11 Consider anonymising data or using separate keys/codes so that the data subject cannot be identified.

8.12 Do not save personal data to your own personal computers or other devices.

8.13 Personal data should never be transferred outside the European Economic Area except in compliance with the law and authorisation of Mariana Dumitru.

8.14 You should lock drawers and filing cabinets. Do not leave paper with personal data lying about.

8.15 You should not take personal data away from Company's premises without authorisation from your line manager or Mariana Dumitru.

8.16 Personal data should be shredded and disposed of securely when you have finished with it.

8.17 You should ask for help from Mariana Dumitru if you are unsure about data protection or if you notice any areas of data protection or security we can improve upon.

8.18 Any deliberate or negligent breach of this policy by you may result in disciplinary action being taken against you in accordance with our disciplinary procedure.

8.19 It is a criminal offence to conceal or destroy personal data which is part of a subject access request (see below). This conduct would also amount to gross misconduct under our disciplinary procedure, which could result in your dismissal.

9 Subject access requests

9.1 Data subjects can make a 'subject access request' ('SAR') to find out the information we hold about them. This request must be made in writing to Mariana Dumitru by email (mariana.dumitru@trpsealing.com). If you receive such a request you should forward it immediately to Mariana Dumitru who will coordinate a response.

9.2 If you would like to make a SAR in relation to your own personal data you should make this in writing to Mariana Dumitru by email (mariana.dumitru@trpsealing,com) We must respond within one month unless the request is complex or numerous in which case the period in which we must respond can be extended by a further two months.

9.3 There is no fee for making a SAR. However, if your request is manifestly unfounded or excessive we may charge a reasonable administrative fee or refuse to respond to your request.

10 Your data subject rights

10.1 You have a right to information about what personal data we process, how and on what basis as set out in this policy.

10.2 You should have the right to access your own personal data by way of a subject access request to Mariana Dumitru.

10.3 You can correct any inaccuracies in your personal data. To do you should contact Mariana Dumitru.

10.4 You have the right to request that we erase your personal data where we were not entitled under the law to process it or it is no longer necessary to process it for the purpose it was collected. To do so you should contact Mariana Dumitru.

10.5 While you are requesting that your personal data is corrected or erased or are contesting the lawfulness of our processing, you can apply for its use to be restricted while the application is made. To do so you should contact Mariana Dumitru.

10.6 You have the right to object to data processing where we are relying on a legitimate interest to do so and you think that your rights and interests outweigh our own and you wish us to stop.

10.7 You have the right to object if we process your personal data for the purposes of direct marketing.

10.8 You have the right to receive a copy of your personal data and to transfer your personal data to another data controller. We will not charge for this and will in most cases aim to do this within one month.

10.9 With some exceptions, you have the right not to be subjected to automated decision-making.

10.10 You have the right to be notified of a data security breach concerning your personal data.

10.11 In most situations we will not rely on your consent as a lawful ground to process your data. If we do however request your consent to the processing of your personal data for a specific purpose, you have the right not to consent or to withdraw your consent later. To withdraw your consent, you should contact Mariana Dumitru.

10.12 You have the right to complain to the Information Commissioner. You can do this be contacting the Information Commissioner's Office directly. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk). This website has further information on your rights and our obligations.

11 How to deal with data breaches

11.1 Introduction

11.1.1 The Company collects, holds, processes, and shares personal data, a valuable asset that needs to be suitably protected.

11.1.2 Every care is taken to protect personal data from incidents (either accidentally or deliberately) to avoid a data protection breach that could compromise security.

11.1.3 Compromise of information, confidentiality, integrity, or availability may result in harm to individual(s), reputational damage, detrimental effect on service provision, legislative noncompliance, and/or financial costs.

11.2. Purpose and Scope

11.2.1 The Company is obliged under Data Protection legislation to have in place an institutional framework designed to ensure the security of all personal data during its lifecycle, including clear lines of responsibility.

11.2.2 This policy sets out the procedure to be followed to ensure a consistent and effective approach is in place for managing data breach and information security incidents across the company.

11.2.3 This policy relates to all personal and special categories (sensitive) data held by the Company regardless of format.

11.2.4 This policy applies to all staff. This includes temporary, casual or agency staff and contractors, consultants, suppliers and data processors working for, or on behalf of the company.

11.2.5 The objective of this policy is to contain any breaches, to minimise the risk associated with the breach and consider what action is necessary to secure personal data and prevent further breaches.

11.3. Definitions / Types of breach

11.3.1 For the purpose of this policy, data security breaches include both confirmed and suspected incidents.

11.3.2 An incident in the context of this policy is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately, and has caused or has the potential to cause damage to the company's information assets and/or reputation.

11.3.3 An incident includes but is not restricted to, the following:

11.3.3.1 loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of laptop, USB stick, iPad / tablet device, or paper record);

11.3.3.2 equipment theft or failure;

11.3.3.3 system failure;

11.3.3.4 unauthorised use of, access to or modification of data or information systems;

11.3.3.5 attempts (failed or successful) to gain unauthorised access to information or IT system(s);

11.3.3.6 unauthorised disclosure of sensitive / confidential data;

11.3.3.7 website defacement;

11.3.3.8 hacking attack;

11.3.3.9 unforeseen circumstances such as a fire or flood;

11.3.3.10 human error;

11.3.3.11 ‘blagging’ offences where information is obtained by deceiving the organisation who holds it.

11.4. Reporting an incident

11.4.1 Any individual who accesses, uses or manages the company’s information is responsible for reporting data breach and information security incidents immediately at mariana.dumitru@trpsealing.com and IT (at mike.evans@trpsealing.com).

11.4.2 If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable.

11.4.3 The report must include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, if the data relates to people, the nature of the information, and how many individuals are involved. An Incident Report Form should be completed as part of the reporting process (refer to Appendix 1).

11.4.4 All staff should be aware that any breach of Data Protection legislation may result in the Company’s Disciplinary Procedures being instigated.

11.5. Containment and recovery

11.5.1 The company will firstly determine if the breach is still occurring. If so, the appropriate steps will be taken immediately to minimise the effect of the breach.

11.5.2 An initial assessment will be made by the Mariana Dumitru/Mike Evans in liaison with relevant officer(s) to establish the severity of the breach and who will take the lead investigating the breach, as the Lead Investigation.

11.5.3 The Lead Investigation Officer (LIO) will establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause.

11.5.4 The LIO will establish who may need to be notified as part of the initial containment and will inform the police, where appropriate.

11.5.5 The LIO, in liaison with the relevant officer(s) will determine the suitable course of action to be taken to ensure a resolution to the incident.

11.6. Investigation and risk assessment

11.6.1 An investigation will be undertaken by the LIO immediately and wherever possible, within 24 hours of the breach being discovered/reported.

11.6.2 The LIO will investigate the breach and assess the risks associated with it, for example, the potential adverse consequences for individuals, how serious or substantial those are and how likely they are to occur.

11.6.3 The investigation will need to take into account the following:

11.6.3.1 the type of data involved;

11.6.3.2 its sensitivity;

11.6.3.3 the protections are in place (e.g. encryptions);

11.6.3.4 what has happened to the data (e.g. has it been lost or stolen;

11.6.4.5 whether the data could be put to any illegal or inappropriate use;

11.6.4.6 data subject(s) affected by the breach, number of individuals involved and the potential effects on those data subject(s);

11.6.4.7 whether there are wider consequences to the breach.

11.7. Notification

11.7.1 The LIO, in consultation with relevant colleagues will establish whether the Information Commissioner's Office will need to be notified of the breach, and if so, notify them within 72 hours of becoming aware of the breach, where feasible.

11.7.2 Every incident will be assessed on a case by case basis; however, the following will need to be considered:

11.7.2.1 whether the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms under Data Protection legislation;

11.7.2.2 whether notification would assist the individual(s) affected (e.g. could they act on the information to mitigate risks?);

11.7.2.3 whether notification would help prevent the unauthorised or unlawful use of personal data;

11.7.2.4 whether there are any legal / contractual notification requirements;

11.7.2.5 the dangers of over notifying; not every incident warrants notification and over notification may cause disproportionate enquiries and work.

11.7.3 Individuals whose personal data has been affected by the incident, and where it has been considered likely to result in a high risk of adversely affecting that individual's rights and freedoms, will be informed without undue delay. Notification will include a description of how and when the breach occurred and the data involved. Specific and clear advice will be given on what they can do to protect themselves, and include what action has already been taken to mitigate the risks.

Individuals will also be provided with a way in which they can contact the company for further information or to ask questions on what has occurred.

11.7.4 The LIO must consider notifying third parties such as the police, insurers, banks or credit card companies, and trade unions. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

11.7.5 A record will be kept of any personal data breach, regardless of whether notification was required.

11.8. Evaluation and response

11.8.1 Once the initial incident is contained, the LIO will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken.

11.8.2 Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

11.8.3 The review will consider:

11.8.3.1 where and how personal data is held and where and how it is stored;

11.8.3.2 where the biggest risks lie including identifying potential weak points within existing security measures;

11.8.3.3 whether methods of transmission are secure; sharing minimum amount of data necessary;

11.8.3.4 staff awareness;

11.8.3.5 implementing a data breach plan and identifying a group of individuals responsible for reacting to reported breaches of security.

11.8.4 If deemed necessary, a report recommending any changes to systems, policies and procedures will be considered by the company.

11.9. Policy Review

This policy will be updated as necessary to reflect best practice and to ensure compliance with any changes or amendments to relevant legislation.

APPENDIX 1

DATA BREACH REPORT FORM

Please act promptly to report any data breaches. If you discover a data breach, please notify Mariana Dumitru/Mike Evans immediately, complete Section 1 of this form and email it at mariana.dumitru@trpsealing.com and IT at mike.evans@trpsealing.com where appropriate.

Section 1: Notification of Data Security Breach	
Date incident was discovered:	
Date(s) of incident:	
Place of incident:	
Name of person reporting incident:	
Contact details of person reporting incident (email address, telephone number):	
Brief description of incident or details of the information lost:	
Number of Data Subjects affected, if known:	
Has any personal data been placed at risk? If, so please provide details:	
Received by:	
On (date):	
Forwarded for action to:	
On (date):	
Received by:	
On (date):	
Section 2: Assessment of Severity	
Details of the IT systems, equipment, devices, records involved in the security breach:	
Details of information loss:	
What is the nature of the information lost?	
How much data has been lost? If laptop lost/stolen:	
How many data subjects are affected?	
Is the data bound by any contractual security arrangements?	
Section 3: Action taken	
Notification to ICO YES/NO	If YES, notified on:
Notification to data subjects YES/	NO If YES, notified on: