TUDOR Business Services Ltd

Data Protection Policy

Introduction

The Processing of Personal Data is essential to the functioning of Tudor and is fundamental to our business.

Words with Capital Letters in this policy denote a defined term. These are set out in Appendix A of this policy.

“Tudor” means: “all companies which are owned or controlled by the Tudor brand”. For a full list of these companies please contact info@tudorltd.com

This data protection policy is designed to promote consistent standards and practices in handling Personal Data across Tudor. This policy requires those who collect and use Personal Data to be open about how it is used, to follow certain principles of good information handling and to respect individual’s rights.

Legal Obligations

Tudor is required to comply with the following laws when Processing Personal Data (*referred to in this Policy as “the Acts”):*

- The Data Protection Act 1998 in the UK
- The Data Protection Act 1988 & the Data Protection (Amendment) Act 2003 in the ROI
- The Privacy and Electronic Communication Regulations 2003 and 2011 and the European Communications (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 in the ROI

Failure to comply could result in serious consequences, including criminal liability for the applicable Tudor company, its directors and individual employees – this includes prison sentences and fines – both at an organisational and individual level. Negligent, reckless or wilful failure of Tudor’s employees to comply with the provisions of this policy will result in action being taken in accordance with Tudor’s disciplinary policy.

Enforcement

The Acts are enforced by the Information Commissioner in the UK and the Data Protection Commissioner in the ROI. All complaints received from the Commissioner’s must be passed to the office immediately.

Scope of this Policy

This policy applies to all Tudor employees in the UK and ROI, both permanent and non-permanent. Tudor has developed the following policies covering specific areas of data protection legislation. These policies are located in the main office.

- Appointing Suppliers
- Data Retention and Destruction

What does this policy mean to me?
The aim of this policy is to ensure that Tudor meets its legal obligations; follows best practice and maintains the quality and reliability of Personal Data.

- All managers are responsible for ensuring that employees and contractors are made fully aware of and comply with the Tudor Group policies and procedures relating to data protection. This includes business procedures within their Office relating to the handling, disclosure and disposal of Personal Data.

- All employees have responsibilities under this policy for ensuring Tudor's compliance with the Acts. Tudor has provided training on data protection and all employees are responsible for ensuring they attend and take all appropriate training provided.

Handling Personal Data
Sections 1 to 4 below describe the approach that Tudor expects you to adopt when handling Personal Data

1) Collecting and using Personal Data fairly

- When collecting Personal Data from individuals, you need to tell them how their information will be used and who will have access to it. Ideally, you should do this at the point you collect the Personal Data. If this is not possible, you should provide the information as soon as possible.

- In some cases, it will be obvious why you have collected the information and you will not need to go through this step, for example where someone gives you their telephone number and asks you to contact them to talk about a Tudor product or service. Where it is not obvious, you need to give people more information. Also, you should not collect information for one reason and use it for a completely unconnected reason, this would clearly be outside that individual's expectations.

- At Tudor, we provide this information to our customers through our Tudor prescribed privacy notices which lets individuals know how we will use their information and who we will disclose it to. For our employees, we provide this detail in your employment contracts. This meets our legal obligations and ensures that our customers and employees understand what is happening to their Personal Data.

- Certain Personal Data is classed as Sensitive under the Acts and you will usually need the express consent of the individual before collecting this type of information.

Further information on collecting and using Personal Data fairly can be found in Tudor's Data Collection policy. Alternatively you can contact the main office.

2) Ensuring the quality of personal data

- At Tudor, we want to ensure that all of the Personal Data we deal with is of good quality. This is simply using common sense and will ensure that we remain compliant with the Acts. We want the information we hold to be adequate and relevant so it is useful to us.

- Personal Data that is inaccurate or out of date is of no use to TUDOR and it will waste the valuable time of our employees following up leads that do not exist anymore.

- Neither should we hold too much information just because it's nice to have. This is especially relevant where you can add free text comments.

- You are reminded that an individual has the right of access to any information written in such a field so you should that ensure all comments are factual.

- Retention of Personal Data needs to be compliant with the Acts. Employees are required to follow Tudor's Data Retention and Destruction Policy, available in the main office

3) Dealing with Individuals' Rights

- Individuals have a number of specific rights under the Acts and Tudor must be able to respond promptly to any requests we receive. These are the most common rights that may be asserted:

Subject Access Request (SAR)

- Subject to a few limited exceptions, individuals are entitled to access any of their Personal Data that is held by Tudor. They may make a request for copies of the Personal Data that Tudor holds on them. Tudor is required to respond to subject access requests within 40 days of receipt of such request.

- SARs may not always be immediately addressed to the main office. Therefore each individual in Tudor is responsible for ensuring that it knows what a SAR is and follow Tudor's Policies.

Requests to Stop Processing for Marketing Purposes

- Individuals have the right to prevent or stop their Personal Data being processed for direct marketing. Tudor will, upon a request from an individual, cease Processing his or her Personal Data for the purpose of direct marketing. All employees are responsible for ensuring individuals' wishes not to receive marketing are actioned and complied with

Prevention of Processing Causing Damage or Distress

- Individuals have the right to prevent their Personal Data being processed where such Processing causes or is likely to cause damage or distress. Such requests must be in writing and must be forwarded to the main office.

4) Keeping Personal Data secure

- Tudor will ensure that the appropriate technical, logical, physical, organisational and operational security measures are in place to ensure the security of Personal Data against unauthorised or unlawful Processing or access and against the accidental loss, destruction or damage to Personal Data.

- Employees should exercise caution when disclosing Personal Data via email or telephone. In particular, you should check the requesting person's identity to make sure the information is only given to someone entitled to it. Do not provide any information if you are uncertain about the requestor's identity.

Reporting Incidents
If you become aware of any breach or potential breach/risk of this Policy, for example, the loss of Personal Data or attempts to obtain Personal Data by deception, you must immediately report this to the office in accordance with Tudor's Policies.

Disclosures to third parties working on our behalf
Tudor has a process for appointing suppliers to process Personal Data on our behalf. This process is outlined in Tudor's Policy on Appointing Suppliers.

Sending Personal Data out of the UK and/or ROI
There are restrictions on sending personal data outside the European Economic Area (the EU Member states plus Norway, Liechtenstein and Iceland). Any employee wishing to transfer Personal Data outside of the EEA, must seek guidance from the Data Protection Office prior to taking such action, in order that the appropriate safeguards can be established.

Who to contact about this Policy?
Any questions regarding this Policy should be directed to your Data Protection Co-ordinator or the main office.

Appendix A – Responsibilities for Personal Data Management

Tudor Executive
The members of the Tudor Executive are collectively responsible for data protection compliance.

Data Governance Committee ("DGC")
The Data Governance Committee ("DGC") is responsible for overseeing compliance with data protection legislation on behalf of the Executive. The Chief Executive sponsors the DGC and a member of Tudor Executive team is appointed as the chair.

DGC Members
The members are responsible for an Office which plays a leading and decision-making role in Tudor's data protection compliance strategy.

Data Protection Co-ordinators
Each business Office throughout Tudor will appoint a Data Protection Co-ordinator (DPC) to be responsible for:

- being the initial contact point within their office for data protection queries
- maintaining awareness of Personal Data Processing activities within their office
- assisting the main office in identification and development of tailored compliance policies and procedures to meet and embed compliance within their office
- assisting the main office in identification of training requirements within their office
- notifying the main office of proposed changes to Personal Data or processes within their office

Appendix B – Definitions

Personal Data - means any information relating to a living individual who can be identified from that information – either on its own or when put together with other information that Tudor holds.

Examples of Personal Data held by Tudor are: names, addresses, telephone numbers, bank account details, appraisals, etc.

Processing - means obtaining, recording or holding the information or data or carrying out any operation or set of operations on Personal Data, including (but not limited to) –

- Organisation, adaptation or alteration of the data,
- Retrieval, consultation or use of the data,
- Disclosure of the data by transmission, dissemination or otherwise making it available, or
- Alignment, combination, blocking, erasure or destruction of the data.

Sensitive Personal Data – means Personal Data consisting of information relating to-

a. racial or ethnic origin,
b. political opinions,
c. religious beliefs or other beliefs of a similar nature,
d. trade union membership,
e. physical or mental health or condition,
f. sexual life,
g. The commission or alleged commission of any offence, or
h. Any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.