Securing the things that are precious to you!

SECURITY MASTERS LIMITED
DATA PROTECTION POLICY

INTRODUCTION

This UK Data Protection Policy (the "Policy") sets out how **Security Masters Limited** (referred to in this Policy us as "we", "us", "our") seeks to protect personal data and ensure staff understand the rules governing their use of personal data to which they have access in the course of their work. In particular, this Policy requires staff to ensure that our **Data Protection Authorised Person** (details can be found under "Key Contacts") should be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

SCOPE

This Policy applies to all staff, contractors, third parties and any other individuals who process personal data on our behalf ("Staff"). You must be familiar with this Policy and comply with its terms.

We may supplement or amend this Policy by additional policies and guidelines from time to time. Any new or modified Policy will be circulated to staff before being adopted.

Who is responsible for this Policy?

The compliance manager **Mark Radford** who has overall responsibility for this Policy. They are responsible for ensuring this Policy is adhered to by all staff.

FALIURE TO COMPLY WITH THIS POLICY

We take compliance with this Policy very seriously. Failure to comply puts both you and the **Security Masters Limited** at risk. The importance of this Policy means that failure to comply with any requirement may lead to disciplinary action under our procedures, which may result in dismissal. In the case of third party service providers it may lead to the termination of our contract with you.

Any employee who considers that the Policy has not been followed by another member of staff or believes that another member of staff may be involved in a security breach should raise the matter with his/her line manager.

If you have any questions or concerns about anything in this Policy, do not hesitate to contact **Mark Radford.**

1. OUR ESTABLISHMENT

Our main establishment is determined according to where we exercise effective and real exercise of management activities determining the main decisions as to the purposes and means of processing through stable arrangements. That criterion does not depend on whether the processing of personal data is carried out at that location. The presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute a main establishment and are therefore not determining criteria for a main establishment.

2. DATA WE PROCESS

A list of the key definitions can be found in Appendix 1. We ask that you familiarise yourself with these key definitions before reading this Policy.

We hold personal data about our employees, clients, suppliers and other individuals for a variety of business purposes e.g. personnel, administrative, financial, regulatory, payroll and business development purposes including the following:

- compliance with our legal, regulatory and corporate governance obligations and good practice
- gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests
- ensuring business policies are adhered to (such as policies covering email and internet use)
- operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information, security vetting, credit scoring and checking
- investigating complaints
- checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments
- monitoring staff conduct, disciplinary matters
- marketing our business
- advertising
- improving services
- accounts and records
- research

As part of our business activity we process **Personal data**, that is information relating to identifiable individuals, such as job applicants, current and former employees, agency, contract, terms and conditions and other staff, clients, suppliers and marketing contacts. Personal data we gather may include: individuals' contact details, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, client materials, invoices and credit card payments.

3. THE PRINCIPLES

As we are responsible for and must be able to demonstrate compliance with the data protection requirements which apply to **Security Masters Limited**, we adhere, and require our Staff to adhere to the principles of data processing, which in summary require that data must:

- be processed fairly and lawfully and shall not be processed unless certain conditions are met.
- be collected for specified, explicit and legitimate purposes and not further processed in a manner

that is incompatible with those purposes.

- be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').

- be 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 ('accuracy');).

- be processed in accordance with the data subject's rights.

- be 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 ('storage limitation');

- be 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 ('integrity and confidentiality')

- not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

These principles apply to obtaining, handling, processing, transportation and storage of personal data. Our Staff who obtain, handle, process, transport and store personal data for us must adhere to these principles at all times.

4. FAIR , TRANSPARENT AND LAWFUL PROCESSING

4.1. ESTABLISHING A LAWFUL GROUND FOR THE PROCESSING OF PERSONAL DATA

Any processing of personal data should be lawful and fair. It should be transparent to those persons whose data we process how their personal data will be collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed.

The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used.

We have an obligation to ensure that we inform individuals of the risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing. In particular, this requires us to ensure that:

- the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data

- the personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed

- the period for which the personal data are stored is limited to a strict minimum

- personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means

- establishing time limits for erasure or for a periodic review

- taking every reasonable step to ensure that personal data which are inaccurate are rectified or deleted

- personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing

4.1.1. Grounds for Processing

We must process personal data fairly and lawfully in accordance with individuals' rights. This generally means that we should not process personal data unless:

- the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

- the processing is necessary:
  - to perform legal obligations, entering into a contract or exercise legal rights, or
  - for compliance with a legal obligation to which the controller is subject; processing is necessary in order to protect the vital interests of the data subject or of another natural person;
  - for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
  - for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

In most cases this provision will apply to routine business data processing activities.

Where we are not basing our grounds for processing on consent or by law in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, we much take into account:

- any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
- the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
- the possible consequences of the intended further processing for data subjects;
- the existence of appropriate safeguards, which may include encryption or pseudonymisation.

4.1.2. Consent

Where our processing is based on the data subject's consent, we must be able to demonstrate that the data subject has given consent to the processing operation and the extent to which consent is given.

This means that consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include:

- ticking a box when visiting an internet website,
- choosing technical settings for information society services or
- another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data.

Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

Where we use consent, capture forms should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.

4.1.2.1. Health Related Data

Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes information about the natural person collected in the course of the registration for, or the provision of, health care, information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test.

4.1.2.2. Withdrawing Consent

Data subjects have the right to withdraw their consent at any time. We have to ensure that it is readily accessible for individuals to be able to withdraw their consent. The withdrawal of their consent does not affect the lawfulness of processing based on consent before its withdrawal.

4.1.3. Relying on our Legitimate Interests

Our legitimate interests, including those to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller.

Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller. We must carefully consider whether a data subject can reasonably expect at the time and in the context of the collection of personal data.

You must contact our Data Protection Authorised person if seeking to rely on a legitimate interest to process data, prior to commencing such data processing activities.

4.1.4. Fraud Prevention

The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned. The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.

4.2. WHAT INFORMATION MUST WE PROVIDE TO DATA SUBJECTS?

When we collect personal data, at the time when personal data are obtained, we need to provide the data subject with all of the following information:

- the identity and the contact details of the controller and, where applicable, of the controller's representative;
- the contact details of the data protection authorised person where applicable; the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- the legitimate interests pursued by the controller or by a third party;

- the recipients or categories of recipients of the personal data, if any;

- where applicable, the fact that the controller intends to transfer personal data to a third country, reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

- the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

- the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;

- the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

- the right to lodge a complaint with a supervisory authority;

- whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

- the existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

4.3. Processing Data for New Purposes

Where we want to make use of personal data which we hold for a purpose other than those for which the personal data were initially collected, we can only do this where the processing is compatible with the purposes for which the personal data were initially collected. If we fall within this category, no legal basis separate from that which allowed the collection of the personal data is required.

In order to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data are initially collected, we have to take into account:

- any link between those purposes and the purposes of the intended further processing;
- the context in which the personal data have been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to their further use;
- the nature of the personal data;
- the consequences of the intended further processing for data subjects; and
- the existence of appropriate safeguards in both the original and intended further processing operations.

If we cannot establish these grounds apply, we must seek consent for new processing activities prior to that further processing with information on that other purpose and other necessary information. In such circumstances, we have to provide this information:

- within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;
- if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or
- if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

Unless:

- the data subject already has the information;
- the provision of such information proves impossible or would involve a disproportionate effort,
- obtaining or disclosure is prohibited for legal reasons
- where the personal data must remain confidential subject to an obligation of professional secrecy.

5. ANONYMISATION AND PSYEUDONOMYMISATION

5.1. Anonymisation

The principles of data protection do not apply anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.

5.2. *Pseudonymisation*

Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person.

To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly.

To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.

The application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations.

5.3. Online Identifiers

Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them. If an individual can be identified from the online identifiers we use them we must treat this as personal data and apply the principles contained within this policy to hem.

6. MARKETING

Where we undertake direct marketing activity we must comply with the Privacy and Electronic Communications Regulations 2003. Under Privacy and Electronic Communications (EC Directive) Regulations 2003 (**PECR**), a company cannot send direct electronic marketing communications (e.g. by telephone, fax, text and email) to individuals who have not specifically opted in to receive it.

Please note that at the time of drafting this Policy the E-Privacy Regulations (which will replace PECR) are still in the process of being negotiated at European Level. As and when the text is agree this policy will be updated accordingly.

7. AUTOMATED DESCISION MAKING AND PROFILING

Individuals have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects

concerning him or her or similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention.

Such processing includes 'profiling' that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her.

We can only undertake such profiling if expressly authorised by law e.g. for fraud and tax-evasion monitoring, or necessary for the entering or performance of a contract between the data subject and a controller, or when the data subject has given his or her explicit consent. In any case, our processing activities should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision. Such measure should not concern a child.

8. ACCURACY AND RELEVANCE

We must ensure that any personal data we process is accurate, adequate, relevant and not excessive given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform **Mark Radford.** We have a duty to investigate such matters.

9. ACCESS TO PERSONAL DATA

All individuals have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing.

9.1. What information may be requested

Data subjects have the right to obtain from us confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

- the purposes of the processing;
- the categories of personal data concerned;
- the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
- where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- the right to lodge a complaint with a supervisory authority;
- where the personal data are not collected from the data subject, any available information as to their source;

- the existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
- Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards that we have put in place.

9.2. What we must provide

If we are a data controller of the data in question, we must provide a copy of the personal data undergoing processing. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

We have a duty to provide the data:

- in a concise, transparent, intelligible and easily accessible form, using clear and plain language.
- in writing, or by other means, including, where appropriate, by electronic means.

9.3. Charing a fee

We must provide information relating to the initial request free of charge. We may charge a reasonable administrative fee for any further copies requested by the data subject. See also manifestly unreasonable requests below.

9.4. Verifying the Identity of the requestor

We must use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services. If we are not satisfied that we have been able to establish the identity of the requestor we may refuse to comply with the request until such time as we can successfully identify the requestor.

9.5. Timescales for compliance

We must provide the information requested without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. We must inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

9.6. Unreasonable requests

Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, we may either:

- charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or
- refuse to act on the request.

We bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

9.7. Where to send requests

If you receive a request you must not respond to, acknowledge or reply in any way to it. Any member of staff who receives a written request should forward it to Mark Radford immediately.

Subject access requests from individuals should be made by e-mail or in writing and addressed to the Data Protection Authorised person **Mark Radford at info@securitymasters.net** or sent to **Mark Radford** at Security Masters Limited Security Masters Ltd. Po Box 61661, London SE9 9AP

10. INDIVIDUALS RIGHT TO ERASURE

Data subjects have the right to have personal data concerning him or her rectified and a 'right to be forgotten' where the retention of such data infringes the law to which the controller is subject. In particular, a data subject has the right to have his or her personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her, or where the processing of his or her personal data does not otherwise lawful. Please note that this right is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet.

The further retention of the personal data should be lawful where it is necessary, for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims.

To strengthen the right to be forgotten in the online environment, the right to erasure extends to situations where we have made the data available to other controllers and must inform the other controllers which are processing such personal data to erase any links to, or copies or replications of those personal data. In doing so, we must take reasonable steps, taking into account available technology and the means available to the controller, including technical measures, to inform the controllers which are processing the personal data of the data subject's request.

Methods by which to restrict the processing of personal data could include, temporarily moving the selected data to another processing system, making the selected personal data unavailable to users, or temporarily removing published data from a website. In automated filing systems, the restriction of processing should in principle be ensured by technical means in such a manner that the personal data are not subject to further processing operations and cannot be changed. The fact that the processing of personal data is restricted should be clearly indicated in the system.

11. INDIVIDUALS RIGHT TO DATA PORTABILITY

Individuals have a right to right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

- the processing is based on consent pursuant or on a contract; and
- the processing is carried out by automated means.

Please note that in exercising his or her right to data portability, individuals have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

12. RIGHT TO OBJECT TO PROCESSING AND AUTOMATED INDIVIDUAL DESCISION MAKING

Individuals have a right to object, to being subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

This right does not apply where the processing is:

- is necessary for entering into, or performance of, a contract between the data subject and a data controller;
- is authorised by law; or
- is based on the data subject's explicit consent.

We must make sure that we have in place suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

12.1. Where to send requests

If you receive a request you must not respond to, acknowledge or reply in any way to it. Any member of staff who receives a written request should forward it to Mark Radford immediately.

13. PROVIDING INFORMATION TO THIRD PARTIES

Any member of staff dealing with enquiries from third parties should be careful about disclosing any personal information held by us. In particular they should:

- Check the identity of the person making the enquiry and whether they are legally entitled to receive the information they have requested.

- Suggest that the third party put their request in writing so the third party's identity and entitlement to the information may be verified.

- Refer to Mark Radford for assistance in difficult situations.

- Where providing information to a third party, do so in accordance with the data protection principles referred to in Section 1.

13.1. OUTSOURCING

13.1.1. Engaging third party processors

Where third parties process personal data on our behalf, such processing shall be governed by a contract or other legal act, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:

- processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

- ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

- takes into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;

- assists us controller in ensuring compliance with these obligations, taking into account the nature of processing and the information available to the processor;

- at our direction, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless the law requires storage of the personal data;

- makes available to us all information necessary to demonstrate compliance with these obligation and allows for and contributes to audits, including inspections, conducted by the controller or another auditor mandated by us.

- contains an indemnity which covers breaches of the written contract.

13.1.2. Sub-Processing

Where our outsourced processors engage another processor for carrying out specific processing activities to fulfil the contract that they have with us, the same data protection obligations as set out in the contract or other legal act between the controller and the processor must be imposed on that other processor by way of a contract or other legal act, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

You must therefore check to see if the contracts we enter into contain prohibitions on sub-contracting and must ensure that the processor flows down the requirements above to their sub-contractors and remain liable for the actions of their sub-contractors. Please contact the Mark Radford for further advice.

14. ASSESSING THE IMPACT OF OUR PROCESSING ACTIVITIES AND CARRYING OUT PRIVACY IMPACT ASESSMENTS

You must seek the advice of our Mark Radford, where designated, when carrying out a data protection impact assessment.

In order to enhance compliance where processing operations are likely to result in a high risk, we are responsible for the carrying-out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of that risk. The outcome of the assessment should be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data complies with the law.

A data protection impact assessment shall in particular be required in the case of:

- a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
- a systematic monitoring of a publicly accessible area on a large scale.

The assessment shall contain at least:

- a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
- an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and
- the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

Where necessary, we shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.

15. DATA SECURITY

In order to maintain security we must evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption. Those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected. In assessing data security risk, consideration should be given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage.

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, we must implement (and ensure out pacers implement) appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

- the ability to ensure the on-going confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

The need to ensure that data is kept securely means that precautions must be taken against physical loss or damage, and that both access and disclosure must be restricted.

All staff are responsible for ensuring that any personal data which they hold is kept securely and that personal information is not disclosed either orally or in writing or otherwise to any unauthorised third party. Failure to comply with our policies and compliance with staff duties of confidentiality may result in disciplinary action that may result in dismissal.

Further information about our technical safeguards and employees' responsibilities in relation to data security are controlled by our IT company Transpeed.

Where other organisations process personal data as a service on our behalf (e.g. payroll or outsourcing companies), **Mark Radford** will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third party organisations. You must not enter into such contracts without obtaining permission to proceed from **Mark Radford.**

16. TRANSFER OF DATA OUTSIDE THE EEA

Security Masters Limited do not proceed to transfer data out of the EEA.

17. RETENTION AND DISPOSAL OF DATA

Information will be kept in line with HMRC's guidelines and legal requirements. All employees are responsible for ensuring that information is not kept for longer than necessary.

Documents containing any personal information will be disposed of securely in our confidential waste bins, and paper copies will be shredded. Staff must not leave confidential materials on their desks. This is especially important in relation to price sensitive transactions or highly confidential matters. Failure to follow this Policy in such circumstances will be considered a serious matter and may result in disciplinary action.

18. OFFSITE WORKING AND COMMUNAL AREAS

Whenever you are working away from the secure areas of the firm's offices, you need to be alert to protect client confidentiality. This affects any areas where third parties could be present. It is particularly easy and tempting for bored fellow travellers on trains to listen to what you are saying or read what you are working on.

Internally, you need to be careful who may overhear if you are discussing a matter which is subject to an information barrier and find a separate area to work in/take a telephone call if need be.

The risks and reputational damage that could come from leaving files unattended are obvious. The easiest things to misplace are discs, memory sticks, slim bundles of paper etc but it's far from unknown for laptops and files to be left behind.

Think:

- about whether you really need to take client or other confidential information, in whatever format, out of the office;
- of where you are and who is there too before you talk about client matters to anyone else;
- whether it is really necessary for you to work on client matters outside of the office - can you be overhead, can someone else read the papers/laptop screen? If you feel uncomfortable, stop work or explain and terminate the call.

Always:

- ensure any confidential information on laptops or memory sticks/discs which you intend to take out of the office is encrypted;
- put papers in a blank file or envelope - if a third party realises from the file label that we act for a certain client, that could be a breach of confidentiality;
- double check to see if anything has been left behind before you leave the place you have been working.

For any further clarification on this please contact **Mark Radford**

19. REPORTING BREACHES

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

- investigate the failure and take remedial steps if necessary
- maintain a register of compliance failures
- notify the Information Commissioners Office if required

Breaches must be reported to Mark Radford <u>immediately</u>. Failure to do so will be considered a serious matter and may result in formal disciplinary action.

REVIEW OF THIS POLICY

Any questions or concerns about the interpretation or operation of this Policy should be taken up in the first instance with the Data Controller, who is responsible for ensuring compliance with the Data Protection Act and implementation of this Policy.

KEY CONTACTS

If you wish to discuss this Policy further please contact:

- Mark Radford

APPENDIX 1

‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

‘restriction of processing’ means the marking of stored personal data with the aim of limiting their processing in the future;

‘profiling’ means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

‘pseudonymisation’ means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

‘filing system’ means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

‘controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

‘processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

‘recipient’ means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

‘third party’ means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

‘consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

‘personal data breach’ means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

‘genetic data’ means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

‘biometric data’ means personal data resulting from specific technical processing relating to the physical, physio logical or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

‘data concerning health’ means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

‘main establishment’ means:

1. (a) as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;
2. (b) as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;

'representative' means a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation;

'enterprise' means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;

'group of undertakings' means a controlling undertaking and its controlled undertakings;

'binding corporate rules' means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;

'supervisory authority' means an independent public authority which is established by a Member State pursuant to Article 51;

'supervisory authority concerned' means a supervisory authority which is concerned by the processing of personal data because:

1. (a) the controller or processor is established on the territory of the Member State of that supervisory authority;
2. (b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or
3. (c) a complaint has been lodged with that supervisory authority;

'cross-border processing' means either:

1. (a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or
2. (b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

'relevant and reasoned objection' means an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data

'international organisation' means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.