GENERAL DATA PROTECTION POLICY

Policy

As a UK established organisation, this policy applies to the processing of personal data regardless of where that processing, or any processing outsourced by us, may take place.

This is an internal policy and it applies to all employees, workers and any other internal persons who may have responsibility for, or have a vested interest in, the operations of the organisation.

Where the organisation does undertake the services of a third party, that party will be required to make adequate assurances to the Data Controller and/or GDPR Owner that their own processing is compliant with current applicable data protection laws.

The policy applies to all data processing in general but particularly to all activities relating to the acquisition, recording, processing, sharing, storing and removal of personal data. In respect of carrying out general business activities, and for illustrative purposes only, such processes include but are not limited to:

- Sales and order processing activities;
- Recruitment activities;
- Collection of marketing data for marketing activities.

Statement

Secon Cyber are committed to engendering a culture of accountability, integrity and confidentiality in all aspects of the organisation regarding personal data and security. Our aim is to align every member of staff to these values such that they may be ambassadors of best practice data processing.

Secon Cyber seek to achieve this by inducting new starters into our security practices and to maintain engagement and commitment to these values through transparent communication, providing regular training to staff and embedding privacy into our practices.
As an employer we process a significant amount of personal data about

REGISTERED IN ENGLAND NO: 3788567
VAT: GB 731672635

SECON CYBER SECURITY LTD

HERSHAM PLACE TECHNOLOGY PARK,
41 - 61 MOLESEY ROAD,
HERSHAM,
SURREY,
KT12 4RZ

PHONE
01932 213 278
SUPPORT
01932 911 053

EMAIL
hello@seconcyber.com

our staff. The type of information we require includes: nationality, date of birth, contact details and medical information. The grounds upon which this information is required will include legal and contractual obligations such as; demonstrating right to work checks, meeting statutory payment conditions and corresponding with individuals in respect of their employment.

Please refer to the section 'Roles and responsibilities' for the details of the Data Controller. For a list of your rights as a data subject, please refer to the section 'The rights of data subjects'.

Principles

All persons who process personal data with our permission must endorse and adhere to these principles at all times and especially when they obtain, handle, process, transfer, store or erase personal data.

The six fundamental principles of personal data processing are as follows:

Fairness, lawfulness and transparency
All personal data must be processed fairly, lawfully, and transparently.

Purpose limitation
All personal data must be collected for specified, explicit and legitimate purposes and shall not be further processed in any manner that is incompatible with those purposes.

Minimisation
All personal data must be adequate, relevant, and limited to what is necessary for the purpose for which they are processed.

Accuracy
All personal data must be accurate and where necessary, kept up to date with regard to the purposes. Every reasonable step to rectify or erase inaccurate personal data must be taken without delay.

Storage limitation
No personal data should ever be kept in a form which permits identification of a data subject for longer than is necessary to achieve the purpose.

Integrity and confidentiality
All personal data must be processed in a manner that ensures appropriate security of the personal data. At the very least, it must always be protected against unauthorised or unlawful processing, accidental loss, destruction or damage, by using appropriate technical and organisational measures.

REGISTERED IN ENGLAND NO: 3788567
VAT: GB 731672635

SECON CYBER SECURITY LTD

HERSHAM PLACE TECHNOLOGY PARK,
41 - 61 MOLESEY ROAD,
HERSHAM,
SURREY,
KT12 4RZ

PHONE
01932 213 278
SUPPORT
01932 911 053

EMAIL
hello@seconcyber.com

The Data Controller is ultimately accountable for each of these principles and is obliged by law to be able to demonstrate compliance. It is for this reason that everyone in the organisation is required to take responsibility for their own strict adherence to these principles.

This policy is not contractual as it may be subject to change. However, it does indicate how we intend to meet our legal responsibilities for data protection. Therefore, any actionable points within it must be regarded as a legitimate management instruction. Explicit permission must always be sought and evidenced from a Line Manager before conducting yourself in a manner that varies from this policy. Failure to do so may result in disciplinary action.

Any additions or revisions to this policy will be communicated to staff where appropriate. We will notify data subjects of any changes that apply to them where appropriate, personally and in writing.

Definitions

Data
Information which is processed or is intended to form part of a filing system. This applies to electronic or hard copy formats.

Data Subject
An identified or identifiable, natural, legal person.

Data Protection Impact Assessments
A Data Protection Impact Assessment (DPIA) (sometimes referred to as a Privacy Impact Assessment (PIA) will be used to ensure privacy by design by conducting a prescribed risk assessment on data processes and making necessary adaptations, thereby implementing appropriate safeguarding measures. A DPIA is made mandatory by law in certain circumstances.

Data Protection Legislation
All privacy laws applicable to any Personal Data processed under or in connection with this Agreement, including, without limitation, the UK Data Protection Act 1998 , the Data Protection Directive 95/46/EC (as the same will be superseded by the General Data Protection Regulation 2016/679 (known as "GDPR")), the Privacy and Electronic Communication Directive 2002/58/EC and all national legislation implementing or supplementing the foregoing and all associated codes of practice and other guidance issued by any applicable Data Protection Authority, all as amended, re-enacted and/or replaced and in force from time to time.

Personal Data (personal information)
Any 'data' relating to a 'data subject' that can be directly or indirectly identified

REGISTERED IN ENGLAND NO: 3788567
VAT: GB 731672635

SECON CYBER SECURITY LTD

HERSHAM PLACE TECHNOLOGY PARK,
41 - 61 MOLESEY ROAD,
HERSHAM,
SURREY,
KT12 4RZ

PHONE
01932 213 278
SUPPORT
01932 911 053

EMAIL
hello@seconcyber.com

by reference to a piece of data. This includes a name, identification number, location data or online identifier. It may be an identifier that relates to physical, physiological, genetic, mental, economic, cultural or social identity. It may also apply to data that has been pseudonymised.

Special category data (sensitive data)
This is also more commonly referred to as 'sensitive data'. In essence this is any data that has the potential to be used to discriminate against a natural person. It includes: racial, ethnic, political opinion, religious or philosophical belief, trade union membership, genetic, biometric data, sex life or sexual orientation data.

It does not include information pertaining to criminal convictions however, such information must be treated with a higher level of security than generic personal data.

Privacy by Design
Privacy by design is the concept of ensuring that security, confidentiality and integrity of personal data is prioritised within the heart of the methods used for processing the data.

Processing
Any activity which is performed on personal data whether or not this is manual or automated, such as: recording, organising, structuring, storing, updating, retrieving, disclosing or erasing. Examples may include: sorting e-mail addresses into categories for marketing campaigns, recording absences from work, monitoring vehicle tracking, etc.

Pseudonymisation
To adapt how personal data is processed and presented such that the data cannot be attributed to a specific data subject, without additional personal data. The additional personal information must be kept separately and securely using appropriate technical and organisational measures.

Recipient
A natural person or organisation to whom personal data is disclosed or otherwise made available. A recipient is not necessarily a third party with whom Secon Cyber has professional dealings.

Roles and Responsibilities

Data Controller

The Role

Secon Cyber's Data Controller is Robert Gupta. His direct contact details are robert.gupta@seconcyber.com .

REGISTERED IN ENGLAND NO: 3788567
VAT: GB 731672635

SECON CYBER SECURITY LTD

HERSHAM PLACE TECHNOLOGY PARK,
41 - 61 MOLESEY ROAD,
HERSHAM,
SURREY,
KT12 4RZ

PHONE
01932 213 278
SUPPORT
01932 911 053

EMAIL
hello@seconcyber.com

Overview of Responsibilities

To be ultimately accountable for Secon Cyber's compliance with the six principles (see section 'Principles').

To be able to demonstrate compliance with the six principles and therefore the proper handling and processing of all personal data. This will include information about the various data protection management resources that have been put into place and take the primary responsibility for the internal data protection framework.

To implement appropriate technical and organisational measures to ensure processing is performed in accordance with data protection laws. These measures will take into account the nature, scope, context and purposes of the data processing and the risks to the rights and freedoms of individuals.

To adopt measures to protect against any high levels of risk identified by a Privacy Impact Assessment, such as; discrimination, identity theft or significant legal, social or economic disadvantage.

To implement internal data protection policies; assign protection responsibilities and to ensure adequate training on data protection is provided and carried out by all staff.

To determine how data subjects may exercise their rights.

Data Protection Officer/ (GDPR Owner)

The Role

The Data Protection Officer role is not required for Secon Cyber for the following reasons:

- The core activities do not require regular and systematic monitoring of data subjects on a large scale.
- Secon Cyber do not process sensitive or special category data.
- Secon Cyber does not operate in the public sector.

The GDPR Owner role is responsible for the arrangement and protection of personal data processed on behalf of and in conjunction with the Data Controller. This role is currently fulfilled by the COO.

Overview of Responsibilities

The responsibilities of the GDPR Owner are:

- To inform and advise the Data Controller and the members of staff who carry out processing, of their obligations under applicable data protection legislation.

REGISTERED IN ENGLAND NO: 3788567
VAT: GB 731672635

SECON CYBER SECURITY LTD

HERSHAM PLACE TECHNOLOGY PARK,
41 - 61 MOLESEY ROAD,
HERSHAM,
SURREY,
KT12 4RZ

PHONE
01932 213 278
SUPPORT
01932 911 053

EMAIL
hello@seconcyber.com

• To monitor compliance with applicable data protection legislation and with the policies of the Data Controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and any related audits.
• To provide advice where requested regarding any DPIAs and to monitor its performance.
• To cooperate with the supervisory authority when necessitated, including any consultation requirements regarding transfers.
• To perform their tasks with due regard to the risks associated with processing operations.
• To not perform any tasks that may result in a conflict of interest.

Conditions for Processing Data

Legal Basis

Under data protection legislation the processing of personal data is prohibited unless there is a legitimate legal basis upon which the data is being processed. There are six potential legal bases for processing.

Legal bases for personal data processing

All persons authorising the processing of personal data must be assured that at least one of the following bases applies:

a) Consent
The data subject must have given consent for specific purposes and be given the option to withdraw consent at any time. Lawful consent may only be obtained if prescribed conditions set out by data protection laws have been met. Consent must always be explicit and may not be implied.

b) Contract
The processing must be necessary to enter in to or adhere to a contract which the data subject is party to. For example, to enter into a contract of employment or when a product or service is purchased by the data subject and personal data is required to provide or perform it.

c) Legal Obligation
The processing must be necessary to comply with a legal obligation that you are bound to. For example, tax obligations, evidencing the right to work or to ensure compliance with the Working Time Directive, etc. Legal obligations imposed by a country outside of the EU may not be justified under this legal basis.

d) Vital Interests
The processing is necessary to protect vital interests of the data subject. For example, subjects who are unable to make decisions in the best interests of

REGISTERED IN ENGLAND NO: 3788567
VAT: GB 731672635

SECON CYBER SECURITY LTD

HERSHAM PLACE TECHNOLOGY PARK,
41 - 61 MOLESEY ROAD,
HERSHAM,
SURREY,
KT12 4RZ

PHONE
01932 213 278
SUPPORT
01932 911 053

EMAIL
hello@seconcyber.com

their health.

e) Public Interest
The processing is necessary to perform a task either in the public interest or under instruction from an official authority or regulatory body. This must be sufficient to reasonably override the interests and rights of the data subjects concerned. It may be used for the defence of a legal claim.

f) Legitimate Interest
The processing must be necessary to pursue a legitimate interest, except where it is overridden by fundamental rights and freedoms of the data subject. (This is not applicable to public authorities.) It is likely to be appropriate where people's data is used in a way in which they may reasonably expect, with minimum impact to their privacy, or where there is a compelling justification for the processing.

Special Category Data
The processing of special category or 'sensitive data' is strictly prohibited under UK and EU data protection laws. There are limited circumstances in which it is permissible to process special category data. If any of the conditions are met, then all other conditions and protections afforded to regular personal data will also apply. Some provisions including security, should be imposed more strictly.

Conditions under which special category data may be processed are:

- The data subject has given explicit consent to the processing of personal data for one or more specified purposes, and there is no overriding legal prohibition.
- Processing is necessary to carry out obligations and specific rights of the Data Controller or of the data subject in the field of employment, social security and social protection law. Appropriate safeguards are imperative.
- Processing is necessary to protect the vital interests of the data subject or of another person who is physically or legally incapable of giving consent. For example, in a medical emergency.
- Processing relates to personal data which are obviously made public by the data subject.
- Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts make instructions to Secon Cyber when acting in their judicial capacity.
- Processing is necessary for reasons of substantial public interest, on the basis of data protection legislation. Advice from the relevant supervisory authority may need to be sought in advance to agree the appropriateness of this condition.
- Processing is necessary for the purposes of the assessment of the working

REGISTERED IN ENGLAND NO: 3788567
VAT: GB 731672635

SECON CYBER SECURITY LTD

HERSHAM PLACE TECHNOLOGY PARK,
41 - 61 MOLESEY ROAD,
HERSHAM,
SURREY,
KT12 4RZ

PHONE
01932 213 278
SUPPORT
01932 911 053

EMAIL
hello@seconcyber.com

capacity of the employee.

Criminal convictions and offences
Personal data of this nature shall be handled with a greater level of protection than that which may be adequate for the processing of standard personal data.

Secon Cyber shall only process data of this nature where there is a legitimate requirement to do so, namely in respect of its duties as an employer. Where there is a legal obligation for Secon Cyber to review or record data of this nature, an appropriate member of staff may seek to establish the required information from the employee, worker, self-employed person, contractor or any other third party.

An example of when this may be necessary is when the performance of a duty requires a criminal record check.

Processing which does not require identification
When processing information, if you can remove all personal data which identifies the data subject, then you will no longer be required to adhere to the conditions for processing detailed in this policy.

If a data subject becomes identifiable then the conditions for processing will apply.

Collecting Data

Transparency Principle
Anyone acting on behalf of Secon Cyber is expressly required to make sure that any information they provide to a data subject or supervisory authority is done so in a manner that is: concise, transparent, intelligible, uses clear and plain language and is provided in an easily accessible form.

Collecting personal data from the subject
If, during the course of your employment, you are required to collect personal data, you must ensure that the data subject is advised or made aware of each of the following:

- The identity and contact details of the Data Controller.
- The contact details of the GDPR Owner.
- The purposes and legal basis of the processing.
- If the legal basis is Secon Cyber's legitimate interest, the interest must be detailed.
- The recipients or categories of recipients of the personal data, if any.
- Whether there is an intention to transfer personal data outside the European Economic Area and if so, whether an adequacy decision by the European

REGISTERED IN ENGLAND NO: 3788567
VAT: GB 731672635

SECON CYBER SECURITY LTD

HERSHAM PLACE TECHNOLOGY PARK,
41 - 61 MOLESEY ROAD,
HERSHAM,
SURREY,
KT12 4RZ

PHONE
01932 213 278
SUPPORT
01932 911 053

EMAIL
hello@seconcyber.com

Commission exists in relation to the transfer, or alternatively reference to the appropriate or suitable safeguards relied upon by Secon Cyber and how these can be obtained.

To ensure fair and transparent processing, the following information must also be provided to the data subject:

- The length of time the personal data will be stored for or the criteria used to determine the length of time it will be stored for.
- Details of their rights.
- Any existence of automated decision-making including profiling, particularly if the profiling produces legal effects or significantly affects a data subject or involves special categories of personal data.
- If you have any questions about any of the above or about the collection or storing of data in general, then please refer to the Data Protection Officer or equivalent.

Collecting personal data from a source other than the subject

When information of this nature is collected, the subject must be provided with all the information in the above clause as well as the information below. This should be provided at the time it is obtained, in concise and plain language.

In these circumstances, the information must be provided within a reasonable period after obtaining the personal data, but at the latest within one month. However, if the data shall be used to communicate with the subject, then the information must have been provided by the first communication. If it shall be disclosed to another party, then the information must have been provided by the first disclosure.

If you acquire personal information in error by any means, you must inform the GDPR Owner immediately and if it is not necessary for you to retain that information, arrange for it to be handled by the appropriate individual in Secon Cyber.

Privacy and Fair Processing Notices

Secon Cyber uses privacy notices to convey the information listed in the sections above at the point of data collection.

The Purpose Changes

If the original purpose for which the data that was collected changes, then the data subject must be informed of the new purpose. They must also be informed of any changes to the information already provided under the points in this section.

REGISTERED IN ENGLAND NO: 3788567
VAT: GB 731672635

SECON CYBER SECURITY LTD

HERSHAM PLACE TECHNOLOGY PARK,
41 - 61 MOLESEY ROAD,
HERSHAM,
SURREY,
KT12 4RZ

PHONE
01932 213 278
SUPPORT
01932 911 053

EMAIL
hello@seconcyber.com

Multiple Data Controllers
In a situation where Secon Cyber should act jointly with other organisations as a Data Controller, then respective responsibilities will be clearly laid out between the parties.

Privacy by Design and Default

It is a legal requirement that all processing of personal data conducted by an organisation is designed to ensure privacy and security of data.

Secon Cyber embeds data protection into the design of every system that uses personal data, so that it is protected throughout its entire lifecycle. To maintain this principle, all members of staff are required to:

- Ensure personal data is mapped, classified into either personal or special category data, labelled, stored and accessible so that it is easily found if need be (e.g. In the event of a subject access request, the need to remove the data or the need to update the data).
- Ensure our systems continue to function so that any personal data that is added may be deleted automatically (where appropriate).
- Ensure that any new documentation which collects personal data is drafted in such a way that no personal data is requested in excess of what is necessary to achieve the purpose.
- Ensure that a data subject is only identified for as long as necessary. This may include removing an identifier such as a name or date of birth.
- Ensure that any new system will process data in a format that is commonly used.

Data Protection Impact Assessments

A Data Protection Impact Assessment (DPIA) must be carried out in respect of processing that is considered likely to put the rights and freedoms of data subjects at a high risk.

A Data Protection Impact Assessment must always be completed if the processing of personal data is likely to be high in risk to the rights and freedoms of the data subject. Examples of processing that may be high risk include systematic monitoring of publicly accessible information on a large scale or profiling that may significantly affect individuals.

Information Security

At Secon Cyber we regularly review our approach to information security and stay up to date with developments in the field and emerging threats. To secure

REGISTERED IN ENGLAND NO: 3788567
VAT: GB 731672635

SECON CYBER SECURITY LTD

HERSHAM PLACE TECHNOLOGY PARK,
41 - 61 MOLESEY ROAD,
HERSHAM,
SURREY,
KT12 4RZ

PHONE
01932 213 278
SUPPORT
01932 911 053

EMAIL
hello@seconcyber.com

the information we hold, we are committed to allocating sufficient resources (including time and budget) to ensure that robust and high-quality tools and processes are implemented.

Secon Cyber takes all reasonable steps to protect and maintain the integrity, confidentiality and availability of personal data. For the purposes of this policy, organisational and technological security measures are in place to protect and secure against:

- Accidental loss
- Damage
- Destruction
- Theft or unsanctioned disclosure
- Publication or transfer of personal data

Key principles are:

a) Protection
All members of staff and any associated third parties are made aware of their responsibilities and are required to exercise and uphold every applicable security measure.

b) Integrity
All members of staff and any associated third parties are made aware of their responsibilities and are required to securely update and maintain completeness of personal data.

c) Confidentiality
All members of staff and any associated third parties are made aware of their responsibilities and are required to only access personal data which they are authorised to process. Those with authority to process personal data will only make personal data available to recipients (other colleagues, third parties etc.) if those recipients are authorised to access or process the data.

d) Availability
Secon Cyber has taken measures to prevent accidental and deliberate unauthorised access. This includes disaster recovery and business continuity arrangements. All members of staff, agency workers and any associated third parties are made aware of their responsibilities and are required to maintain the measures put in place by Secon Cyber to physically and virtually secure information. If they detect any threats to the continued availability of access to assets, systems and information they must report this to a line manager so that it may be escalated appropriately. Threats may include: damage to a computer of filing system, faulty locks, viruses or malware.

REGISTERED IN ENGLAND NO: 3788567
VAT: GB 731672635

SECON CYBER SECURITY LTD

HERSHAM PLACE TECHNOLOGY PARK,
41 - 61 MOLESEY ROAD,
HERSHAM,
SURREY,
KT12 4RZ

PHONE
01932 213 278
SUPPORT
01932 911 053

EMAIL
hello@seconcyber.com

You must not take personal information (including employment records) away from Secon Cyber premises save in circumstances where you have obtained prior consent from the COO or GDPR Owner to do so.

This section is applicable to self-employed persons and contractors in so far as they will be asked to ensure compliance with these points and our security measures. In any event, they will be required to uphold obligations under applicable data protection laws at all times and without exception. Failure to do so will enable Secon Cyber to terminate the service agreement without notice and the incident may be reported to the relevant supervisory authority.

Transferring Personal Data to a Country Outside the EEA

As we may need to transfer personal data outside of the European Economic Area ("EEA"), we have ensured that the following condition applies:

- The transfer is necessary for one of the reasons set out in data protection legislation, including the performance of a contract between the data subject and us, or to protect the vital interests of the data subject.

Subject to this condition, personal data we hold may be processed by staff operating outside the EEA who work for us or for one of our suppliers. These staff may be engaged in, among other things, the fulfilment of contracts with the data subject, the processing of payment details and the provision of support services.

Record Keeping

Secon Cyber will maintain records of data processing activities in accordance with data protection legislation. Record keeping is carried out for the processing of personal data which is regular and frequent.

Breach and Incident Reporting

Serious breaches must be reported to the relevant supervisory authority within 72 hours of becoming aware of the breach. Therefore, all employees and workers must immediately report an incident that may potentially or actually put personal data at risk of a data breach. This is never more imperative than when it is suspected that there may be actual loss, theft unauthorised disclosure or inappropriate use of personal data, either wholly or partly. In this event you must immediately refer to and follow Secon Cyber's Breach and Incident and Reporting Procedure.

Where a third-party service provider notifies you of an incident that may affect Secon Cyber and its responsibilities, you must immediately report the incident. In this event you must immediately refer to and follow Secon Cyber's Breach and

REGISTERED IN ENGLAND NO: 3788567
VAT: GB 731672635

SECON CYBER SECURITY LTD

HERSHAM PLACE TECHNOLOGY PARK,
41 - 61 MOLESEY ROAD,
HERSHAM,
SURREY,
KT12 4RZ

PHONE
01932 213 278
SUPPORT
01932 911 053

EMAIL
hello@seconcyber.com

Incident Reporting Procedure.

The Rights of Data Subjects

Secon Cyber shall be diligent in providing data subjects information about their rights and in complying with any appropriate assertions of their rights.

All reasonable efforts will be made to verify the identity of the data subject before carrying out any requests or disclosures of information made by them. These efforts may include the request for additional personal information if necessary.

The following rights apply to all data subjects:

a) Right of transparent communication
b) Right of access
c) Right to rectification
d) Right to erasure (right to be forgotten)
e) Right to restriction of processing
f) Obligation to notify recipients
g) Right to data portability
h) Right to object
i) Right to not be subject to automatic decision making

Subject Access Requests

If you wish to make a subject access request to verify the lawfulness and accuracy of the personal data we hold about you, then you are encouraged to put your request in writing (letter or e-mail) and submit it to the COO.

Your request should be specific about the nature and the type of data you require.

Every attempt will be made to comply with your request in a timely manner and without undue delay.

Upon receipt of the information you are encouraged to check the accuracy of the information and to advise Secon Cyber of any updates that may need to be made.
A fee will not be charged for an access request, except where a request is deemed to be 'manifestly excessive' or you have already been provided with the information.

Receiving a Request

If you receive a request, you should pass it to the COO.

REGISTERED IN ENGLAND NO: 3788567
VAT: GB 731672635

SECON CYBER SECURITY LTD

HERSHAM PLACE TECHNOLOGY PARK,
41 - 61 MOLESEY ROAD,
HERSHAM,
SURREY,
KT12 4RZ

PHONE
01932 213 278
SUPPORT
01932 911 053

EMAIL
hello@seconcyber.com

Requests must be acknowledged upon receipt.

Requests must be complied with in a timely manner and without undue delay. If it is anticipated that compliance with a request is not going to be immediate, the Data Controller should be notified and informed of the legitimate reasons for this. The information requested must be provided within one month of receipt of the request.

If an extension to the timeline is absolutely necessary under exceptional circumstances, then any extension must be agreed by the data subject and signed off by the Data Controller within one month of the request. If an extension is agreed, then the information must be provided within a maximum of three months from the receipt of the request.

If a request is received electronically (e.g. via e-mail) then the request must be responded to electronically.

The data must be provided in a common format (e.g. a paper file, a pdf document, etc.).

Only personal data pertaining to the individual who made the request should be released.

If there is any doubt over the identity of the individual making the access request, then reasonable steps must be taken to verify their identity, before complying with the request.

When the personal data is provided, the individual must be informed of the right to lodge a complaint with the relevant supervisory authority and the existence of the right to objection, rectification, erasure and restriction of the data.
The data subject may be directed to the relevant privacy/fair processing notice which will provide advice on the conditions for processing.

General Guidance for Employees

We recognise that there are different areas in the organisation where members of staff may be responsible for processing personal data in different ways. We also recognise that responsibilities and nuances in processing are likely to vary across specialisms and levels of seniority.

Secon Cyber will provide guidance to staff when processing personal data specific to their job. This information shall include:

- A description of the limitations which surround how personal data can be used.

REGISTERED IN ENGLAND NO: 3788567
VAT: GB 731672635

SECON CYBER SECURITY LTD

HERSHAM PLACE TECHNOLOGY PARK,
41 - 61 MOLESEY ROAD,
HERSHAM,
SURREY,
KT12 4RZ

PHONE
01932 213 278
SUPPORT
01932 911 053

EMAIL
hello@seconcyber.com

- The steps that must be followed to ensure that personal data is maintained accurately.
- A comprehensive discussion of security obligations, including all reasonable steps that should be taken as a minimum to prevent unauthorised access or loss.
- A signpost to Secon Cyber's Information Security Policy.
- Confirmation of whether the transfer of personal data shall be permitted. Transfer of personal data is prohibited unless specific legitimate grounds have been established.
- Specific information regarding the way in which personal data should be handled when it is destroyed or deleted.

General Responsibilities of Management

All members of the senior management are responsible for championing and enforcing this policy to all other staff within Secon Cyber, whenever appropriate.

Particular roles within senior management are responsible for assessing the business risk arising as a result of processing personal data. These roles include:

- CEO
- COO
- Directors

Those members of senior management identified above are required to work with Secon Cyber to develop procedures and controls to identify and address risks appropriately.

Responsibility will be allocated to individual roles for determining risk-based technical, physical and administrative safeguards including safeguards for equipment, facilities and locations where personal data is stored and establishing procedures and requirements for collecting, transporting, processing, storing, transferring (where appropriate) and destroying personal data. These considerations must also be given when dealing with any third parties who may be authorised or obligated to process personal data on behalf of Secon Cyber.

Non-compliance

This policy, along with associated documents, seeks to guide and instruct all members of staff on how they ensure compliance with data protection laws to which Secon Cyber is subject.

If a member of staff should fail to comply with applicable data protection laws, they may subject Secon Cyber and themselves as individuals to civil and

REGISTERED IN ENGLAND NO: 3788567
VAT: GB 731672635

SECON CYBER SECURITY LTD

HERSHAM PLACE TECHNOLOGY PARK,
41 - 61 MOLESEY ROAD,
HERSHAM,
SURREY,
KT12 4RZ

PHONE
01932 213 278
SUPPORT
01932 911 053

EMAIL
hello@seconcyber.com

criminal penalties. This is likely to jeopardise the reputation of Secon Cyber and as a result may impact on the operational and performance capabilities of the business.

As the ramifications of non-compliance are potentially severe, any failure to comply with this policy or reasonable instruction given in connection with the protection and security of personal data, may result in disciplinary action. Serious, deliberate or negligent transgressions may be regarded as gross misconduct and if substantiated, may result in summary dismissal (without notice).

Third Parties, Contractors, and Self-employed Persons

If any self-employed person, contractor or third party is found to be failing to meet obligations with applicable data protection laws, then notice may be served on the contract for service.

Serious, deliberate or negligent transgressions may permit Secon Cyber to terminate the contract for service with immediate effect. In this event, all reasonable steps will be taken to recover and protect the personal data concerned and the relevant supervisory authority will be notified. Where the rights and freedoms of data subjects are likely to be at risk, the data subjects will be notified without delay.

Breach and Incident and Reporting Procedure

Secon Cyber is committed to the protection of information and has in place a number of technical and organisational measures to safeguard the information it owns. This includes technical security and organisational safeguards ranging from physical building and office security to procedural standards and requirements for the safe handling and storage of information. This procedure covers reporting of actual or suspected data security incidents that may be data breaches.

Purpose

Secon Cyber recognises that from time to time 'things go wrong' and there may be a breach of security involving information or equipment holding information. The purpose of this procedure is to ensure that all actual or potential information security incidents are reported centrally to enable Secon Cyber to react quickly and effectively to minimise the impact.

The aims of the procedure are as follows:

REGISTERED IN ENGLAND NO: 3788567
VAT: GB 731672635

SECON CYBER SECURITY LTD

HERSHAM PLACE TECHNOLOGY PARK,
41 - 61 MOLESEY ROAD,
HERSHAM,
SURREY,
KT12 4RZ

PHONE
01932 213 278
SUPPORT
01932 911 053

EMAIL
hello@seconcyber.com

- Timely advice on containment and risk management
- Determine whether further controls or actions are required
- Consider whether the incident is required to be notified to the individual(s)/ organisations affected by the incident
- Evaluate lessons learnt and areas for improvement

All information security incidents will be dealt with by Secon Cyber 'Incident Group', which comprises of the CEO, COO, Secon Cyber Security and Support Engineers, HR and Head of Marketing with a nominated Incident Lead, who will review and advise on incidents and make recommendations on appropriate follow up and corrective action. Specialist input will be sought from where necessary.

Scope

This procedure applies to all staff. Secon Cyber requires organisations providing services that hold or process personal information on its behalf (i.e. acting as data processors) to have in place internal reporting requirements equivalent to this procedure and for any third party breaches to be reported immediately to Secon Cyber Data Protection Officer in the first instance.

Identifying Incidents

The General Data Protection Regulation (Regulation (EU) 2016/679) defines a data breach as "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". Information security incidents can therefore cover a multitude of situations, but generally it will involve an adverse event which results, or has the potential to result in the compromise, misuse or loss of Secon Cyber owned or held information or assets.

Data breaches can be categorised according to the following three information security principles:

- Confidentiality breach – where there is an unauthorised or accidental disclosure of, or access to, personal data
- Availability breach – where there is an accidental or unauthorised loss of access to, or destruction of, personal data
- Integrity breach – where there is an unauthorised or accidental alteration of personal data.

Information in this procedure is used as a collective term and may include personal or sensitive/ special category personal data as defined under the data legislation (or confidential personal data as commonly referred to in the health sector) and also business information.

REGISTERED IN ENGLAND NO: 3788567
VAT: GB 731672635

SECON CYBER SECURITY LTD

HERSHAM PLACE TECHNOLOGY PARK,
41 - 61 MOLESEY ROAD,
HERSHAM,
SURREY,
KT12 4RZ

PHONE
01932 213 278
SUPPORT
01932 911 053

EMAIL
hello@seconcyber.com

Some examples of information security incidents include (but are not limited to):

- The loss or theft of information or equipment,
- Incorrect handling of protectively marked information,
- Poor physical security,
- Hacking,
- Information disclosed in error,
- Unauthorised use or access to information or systems

The impact of a security incident can vary greatly depending on the type of information or asset involved. It may for instance lead to an infringement of privacy, fraud, financial loss, service disruption or reputational damage. The purpose of reporting an incident is not to apportion blame but to ensure that any impact is minimised and lessons learnt can be identified and disseminated.

The principles of this procedure also apply to cyber incidents i.e. any incident that could or has compromised information assets within the Council's digital network for e.g. phishing emails or hacking attacks. Any cyber-related incident will be handled in accordance with Secon Cyber's Incident Response Procedure by the Delivery Team, headed by the COO.

In the event that a cyber incident also involves a data breach, it shall remain subject to this procedure and the Incident Lead will work in conjunction with Delivery Team to resolve the incident and report to any regulators as necessary.

Reporting Incidents

A direct Line Manager or supervisor should always be made aware of any information security incident and the incident reported in line with this procedure. Informing a Line Manager or supervisor of an incident must not delay any incident being reported under this procedure.

All information security incidents should be reported immediately (and in any event within four hours) after an individual is aware of a potential or actual incident. Informing a Line Manager of an incident must not delay any incident being reported under this procedure.

The person reporting the incident should telephone Secon Cyber's Support number as soon as possible (available from the Website). They will ask questions required to determine the risk and actions to be taken. For the purposes of this procedure, lost or stolen hardware will be logged and may be subject to further investigation depending on the circumstances giving cause to the incident.
The Police should be notified immediately of any incidents involving stolen information or equipment and a crime reference number obtained. It is the responsibility of the individuals who had equipment stolen to notify the police.

REGISTERED IN ENGLAND NO: 3788567
VAT: GB 731672635

SECON CYBER SECURITY LTD

HERSHAM PLACE TECHNOLOGY PARK,
41 - 61 MOLESEY ROAD,
HERSHAM,
SURREY,
KT12 4RZ

PHONE
01932 213 278
SUPPORT
01932 911 053

EMAIL
hello@seconcyber.com

Incident Classification

The severity of an information security incident will be determined in accordance with Secon Cyber's incident levels set out by the Delivery Team.

An incident will be rated in accordance with Secon Cyber's corporate strategy to risk management, which is based on agreed criteria for assessing the likelihood, severity and impact of risk.

Matters to consider would include:

- The nature, sensitivity and volume of personal data;
- Ease of identification of individuals;
- Severity of consequences for individuals;
- The number of affected individuals;
- Nature of breach (e.g. Error, mistake or intentional action and malicious);
- Financial or legal implications and reputational damage.

It is difficult to provide a definitive list of incidents by level as each case varies depending on the circumstances, including containment and recovery, which may reduce or escalate the level at any given point. An initial incident rating will be awarded upon incident notification and may change once the facts and impact of risks has been determined.

Generally the less serious incidents will involve encrypted data or low level data including near misses whereby the severity is reduced due to fortunate events. The more serious incidents will involve high level data which poses actual or potential high risk to people's rights and freedoms or to the organisation e.g. Through the loss or release of highly sensitive personal or confidential business information.

REGISTERED IN ENGLAND NO: 3788567
VAT: GB 731672635

SECON CYBER SECURITY LTD

HERSHAM PLACE TECHNOLOGY PARK,
41 - 61 MOLESEY ROAD,
HERSHAM,
SURREY,
KT12 4RZ

PHONE
01932 213 278
SUPPORT
01932 911 053

EMAIL
hello@seconcyber.com