10. General Data Protection Regulation Policy

Following up on our *2. Client & Confidentiality* Policy; *2.1* and *2.2*, we assure privacy of our clients and security operatives' personal information. We will continue to abide by Art 6.1 GDPR law and apply where is necessary.

A **GDPR** (General Data Protection Regulation) is essential for any business. It is a way to not only protect your information you share with us, but for our company to comply with necessary laws in place. Our compliance follows:

10.1 We DO NOT share sensitive information to any third parties.

10.1.a We do not conduct unlawful practices of data – sharing, buying or profiting.
10.1.b We do not share your data UNLESS requested by appropriate methods of lawful investigation.
10.1.c We do not keep your information beyond an expired contract length;

10.1.c.a Unless you are a long term client or security operative who wishes to continue our agreed exchange of service by reprising contracts.

10.1.c.b You may request and sign a consent form with us permitting we keep your personal information for continuous contracted work.

10.2 We DO keep all our client and security operatives' personal information private.

10. 2.a We do retain relevant information of each individual that we sign under contract, such as; your contact details, SIA license copies, payment information i.e bank account numbers for future assignments with us.
10.2.b We do maintain regular updates of your information with us where necessary and request complete accuracy of information shared.
10.2.c We do comply with your rights to access, retrieve and process your information.

10.3 Your Rights in GDPR

Understanding your rights in GDPR can help you know the relevancy of how and what your information is used for. Here are eight rights you can follow through:

- **Right to be informed**: Your data collected by any organisation, must be transparent in what is processed, how it is used, how long it is kept (e.g. contract length) and whether it will be shared to third parties.

- **Right of access**: You can request a copy of your information that an organisation may have. The organisation or company has one month to produce this information. There are some exceptions for requests if unattested, excessive or repetitive.

- **Right of rectification**: You can request to correct inaccurate or incomplete information. An organisation or company can oblige up to one month duration to do this.

- **Right to erasure**: In certain situations, you can ask an organisation to erase any of your personal data stored. Examples of request for erasure; data is no longer necessary, data is/was unlawfully processed and no longer has lawful ground to validate reasons of being collected or kept – i.e. withdrawing your consent.

- **Right of portability**: You can request a transfer of your data held by the organisation to another company. Your personal data is yours to obtain and reuse across different services of your choice by way of contract or consent.

- **Right to restrict processing**: An alternative to requesting erasure: in specific situations, you can request an organisation to limit its use of your personal data.

- **Right to object**: You can object to the processing of your personal data. You can make an objection either written or verbal allowing a calendar month to response. Organisations are obliged to stop processing information upon immediate request.

- **Rights related to automated decision making, including profiling**: You have the right to object to decisions about you by automated processes or profiling. This means, automated (non-human, algorithmic) profiling calculates assumptions based on your personal data given or shared. You challenge this by requesting a review if you believe the rules aren't being followed.

10.4 Principles

There are 7 GDPR principles which serve as strict guidelines for all organisations and companies to follow through. Here is a guide sourced from ICO (Information Commissioners Office);

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

1. Lawfulness, fairness and transparency

Article 5(1) of the UK GDPR says:

"1. Personal data shall be:
(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness, transparency')"

Three parts explained:

What is lawfulness?

Lawfulness means that you don't do anything with the personal data which is unlawful. This includes statute and common law obligations, whether criminal or civil. If processing involves committing a criminal offence, it will be unlawful. Other unlawful details to keep in check;

- a breach of a duty of confidence;
- an organisation exceeding its legal powers or exercising those powers improperly;
- an infringement of copyright;
- a breach of an enforceable contractual agreement;
- a breach of industry-specific legislation or regulations; or
- a breach of the Human Rights Act 1998.

What are the lawful bases for processing?

The lawful bases for processing are set out in Article 6 of the UK GDPR. At least one of these must apply whenever personal data is processed:

(a) Consent: the individual has given clear consent to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract with the individual, or they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary to perform a task in the public interest or for official functions: the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for legitimate interests of a company/organisation, or the legitimate interests of a third party. Unless there is a good reason to protect the individual's personal data, this then overrides those legitimate interests. (This cannot apply if a public authority is processing data to perform official tasks.)

What is fairness?

Processing of personal data must always be fair as well as lawful. If any aspect of your processing is unfair you will be in breach of this principle – even if you can show that you have a lawful basis for the processing.

Assessing whether you are processing information fairly depends partly on how you obtain it. In particular, if anyone is deceived or misled when the personal data is obtained, then this is unlikely to be fair.

Consider how it affects the interests of the people concerned – as a group and individually.

It will be considered unfair if information is selective to a particular group or person, and the one or the other is not treated in the same lawful process.

Personal data may sometimes be used in a way that negatively affects an individual without this necessarily being unfair. What matters is whether or not such detriment is justified.

What is transparency?

Transparency is fundamentally linked to fairness. Transparent processing is about being clear, open and honest about who the company/organisation is, and how personal data is processed and why.

Individuals must know they have a choice to enter partnerships (sign contracts etc). It helps that transparency allows an individual to make an informed

decision before entering a partnership or agreement and can renegotiate terms of that relationship.

'Invisible processing' is the indirect (third party) collection of personal data. An individual may not know this, and so it is important that any company or organization handling the indirect collection, be transparent. Examples to be aware of; list brokering, direct marketing and online tracking.

2. Purpose Limitation

Article 5(1)(b) says:

"1. Personal data shall be:
(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes."

In practice, this means:

- clear intentions on collecting personal data;
- specifying purpose in compliance with documentation obligations;
- being transparent about data collection;
- specify any plans that is different to the original intention of data collection, and be direct on third party involvement;
- consent given by individual where necessary, if original purpose of data differs and done under lawful means;

A small organisation is exempt from some documentation requirements. Not all formal documentations purposes need to comply with the purpose limitation principle. However, the privacy information should detail the necessary.

3. Data Minimisation

Article 5(1)(c) says:

"1. Personal data shall be:
(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation)"

In practice:

- Identifying the minimum amount of personal data needed on the intended purpose. No more.

- Individuals have the right to complete any incomplete data which is inadequate for company/organisation purpose, under the *right to rectification*. Individuals have the right to delete any data that is not necessary for company/organisation purpose, under the right to erasure (right to be forgotten).

How do we decide what is adequate, relevant and limited?

This will depend on a specified purpose for collecting and using the personal data. It may also differ from one individual to another.

To assess holding the right amount of personal data, a company/organisation must be clear about the why.

For special category data or criminal offence data, it is particularly important to collect and retain only the minimum amount of information.

Consider categorizing each individual, or grouping for specific characterizations.

Consider any specific factors that an individual brings to attention – for example, as part of an objection, request for rectification of incomplete data, or request for erasure of unnecessary data.

A company/organisation periodically reviews the processing of personal data it holds, and retains what is relevant within contractual agreements.

A company/organisation must not collect personal data on the off-chance that it might be useful in the future. However, a company/organisation can only hold onto information if they can justify within reason for unforeseeable events.

4. Accuracy

Article 5(1)(d) of the UK GDPR says:

"1. Personal data shall be:
(d) 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')"

In practice, this means:

- Take reasonable steps to ensure the accuracy of any personal data;
- Ensure that the source and status of personal data is clear;
- Carefully consider any challenges to the accuracy of information; and
- Consider whether it is necessary to periodically update the information.

When is personal data 'accurate' or 'inaccurate'?

The UK GDPR does not define the word 'accurate'. However, the Data Protection Act 2018 does say that 'inaccurate' means "incorrect or misleading as to any matter of fact". It will usually be obvious whether personal data is accurate.

Be clear about what is intended on record (personal data) to show. Personal data must be accurate on all platforms.

Does personal data always have to be up to date?

Depending on what the information is for, if it serves any current purpose, then it needs to be up-to-date. Examples;

- Update employee payroll records when there is a pay rise;
- Update records for customers' changes of address so that goods are delivered to the correct location.

5. Storage Limitation

Article 5(1)(e) says:

"1. Personal data shall be:

(e) 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')"

Personal data cannot be kept for longer than is needed. There is no specific time limits in UK GDPR.

Why is storage limitation important?

Personal data held for too long will, by definition, be unnecessary and there is no lawful basis for retention.

From a more practical perspective, it is inefficient to hold more personal data than needed, and there may be unnecessary costs associated with storage and security.

Good practice around storage limitation:

- Clear policies on retention periods and erasure – this will likely reduce the burden of dealing with queries about retention and individual requests for erasure.

6. Integrity and Confidentiality (security)

Article 5(1) (f) of the UK GDPR concerns the 'integrity and confidentiality' of personal data. It says that personal data shall 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'

Companies and organisations must ensure appropriate security measures are in place to protect the personal data held.

Personal data cannot be accidentally or deliberately compromised.

Information security sometimes considered as cybersecurity (the protection of your networks and information systems from attack), must cover other things like physical and organisational security measures.

This can also be referred to as the 'security principle' and concerns the broad prospect of information security.

What do our security measures need to protect?

The security principle goes beyond the way information is stored or transmitted. Every aspect of processing personal data is covered, not just cybersecurity. This means the security measures put in place should seek to ensure that:

- the data can be accessed, altered, disclosed or deleted only by those who are authorised to do so (and that those selected only act within the scope of the authority given);
- the data held is accurate and complete in relation to its appropriate use;
- the data remains accessible and usable, ie, if personal data is accidentally lost, altered or destroyed, it should be recoverable, and therefore prevent any damage or distress to the individuals concerned.

These are known as 'confidentiality, integrity and availability' and under the UK GDPR, they form part of a company/organisations obligations.

What level of security is required?

The UK GDPR does not define the security measures that a company or organisation should have in place. It requires a level of security that is 'appropriate' to the risks

presented by its processing. Consider this in relation to the state of the art and costs of implementation, as well as the nature, scope, context and purpose of processing.

This reflects both the UK GDPR's risk-based approach, and that there is no 'one size fits all' solution to information security. What's 'appropriate' for a company/organisation will depend on circumstances, the processing you're doing, and the risks it presents to the organisation.

Assessment and review that a company/organisation must take into account considering all aspects of safety:

- the nature and extent of the organisation's premises and computer systems;
- the number of staff and the extent of their access to personal data;
- any personal data held or used by a data processor acting on one's behalf.

What organisational measures to consider?

Clear accountability for security will ensure that issues are not overlooked, and overall security posture does not become flawed or out of date.

Having a policy enables a demonstration on how a company/organisation are taking steps to comply with the security principle.

Considering security and other related matters;

- co-ordination between key persons in the company/organisation;
- access to premises or equipment given to anyone outside the company/ organisation (e.g. for computer maintenance) and the additional security considerations this will generate;
- business continuity arrangements that identify how to protect and recover any personal data held;
- periodic checks to ensure that security measures remain appropriate and up to date.

What technical measures to consider?

Technical measures are the protection of personal data held in computers and networks. Many security incidents can be down to theft or loss of equipment, the abandonment of old computers or hard-copy records being lost, stolen or incorrectly disposed of. Technical measures therefore include both physical and computer or IT security.

When considering *physical security*, look at factors such as:

- the quality of doors and locks, and the protection of premises by such means as alarms, security lighting or CCTV;
- controlled access to premises, and how visitors are supervised;
- disposal of any paper and electronic waste;
- how to keep IT equipment, particularly mobile devices, secure.

In the IT context, technical measures may sometimes be referred to as 'cybersecurity'. This is a complex technical area that is constantly evolving, with new threats and vulnerabilities always emerging. It may therefore be sensible to assume that systems are vulnerable and to take steps to protect them.

When considering *cybersecurity,* look at factors such as:

- ***system security*** – the security of a network and information systems, including those which process personal data;
- ***data security*** – the security of the data held within the systems, e.g. ensuring appropriate access controls are in place and that data is held securely;
- ***online security*** – e.g. the security of your website and any other online service or application that is used; and
- ***device security*** – including policies on Bring-your-own-Device (BYOD) if it is offered.

7. Accountability

The accountability principle requires you to take responsibility for what you do with personal data and how you comply with the other principles.

You must have appropriate measures and records in place to be able to demonstrate your compliance.

What is accountability?

There are two key elements. First, the accountability principle makes it clear that you are **responsible** for complying with the GDPR. Second, you must be able to **demonstrate** your compliance.

Article 5(2) of the GDPR says:

"The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')

Why is accountability important?

A company/organisation that takes responsibility for relevant means of processing personal data, and demonstrating the steps taken to protect people's rights results in better legal compliance, it also offers a competitive edge. Accountability is a real opportunity to show, and prove, the respect a company/organisation respects people's privacy. Developing trust is the core element here.

As a smaller organisation, a smaller scale approach to accountability among other things include:

- ensuring a good level of understanding and awareness of data protection among staff;
- implementing comprehensive but proportionate policies and procedures for handling personal data; and
- kept records of what is done and why.

Article 24(1) of the UK GDPR says:

- must implement technical and organisational measures to ensure, and demonstrate, compliance with the UK GDPR;
- the measures should be risk-based and proportionate; and

- a need to review and update the measures as necessary.

Is it relevant to adopt a 'data protection by design and default' approach?

Under the heading 'data protection by design and by default', the UK GDPR legally requires a company/organisation to take this approach.

Data protection by design and default is an integral element of being accountable. It is about embedding data protection into everything that's done, throughout all processing operations. The UK GDPR suggests measures that may be appropriate such as minimising the data collected, applying pseudonymisation techniques, and improving security features.

Integrating data protection considerations into operations help to comply with obligations, while documenting the decisions made (often in data protection impact assessments).

Relevance to use contracts?

Whenever a controller uses a processor to handle personal data on their behalf, it needs to put in place a written contract that sets out each party's responsibilities and liabilities.

Contracts must include certain specific terms as a minimum, such as requiring the processor to take appropriate measures to ensure the security of processing and obliging it to assist the controller in allowing individuals to exercise their rights under the UK GDPR.

Using clear and comprehensive contracts with processors helps to ensure that everyone understands their data protection obligations and is a good way to demonstrate this formally.

Policies are meant to protect all involved and to communicate our operations and responses. We value our clients, our security operatives and the work we offer. Our policies may change and adapt to the growth of the company as well as concurrent changes in UK laws applicable to security and what is relevant. We thank you and appreciate your time to understand these policies. Please reach out to us for any further questions.

Agreement/Declaration statement:

We believe that the above written policy for WL Risk Management [GDPR – General Data Protection Regulation] is accurate as it is written by law, and represents the compliance and integrity of this company. We take full responsibility to exercise our legal stance should any unintended breaches occur, and we will co-operate with the relevant authorities, specialists and appointed advisors in handling any matters appropriately.

Sign: 

Date:

SignNow e-signature ID: 19c79c3c36...
09/08/2022 11:18:36 UTC

Management [Accounts]: Leihana Volavola

Sign: 

Date:

SignNow e-signature ID: cf30b6c66e...
09/08/2022 11:18:36 UTC

Approval [Director of Operations]: Wame Volavola