General Data Protection Policy

Context and overview

Introduction

Salder Consulting Ltd needs to gather and use certain information about individuals. These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact. This policy describes how this personal data must be collected, handled and stored to meet the Salder Consulting Ltd data protection standards and to comply with the law.

Why this policy exists

This data protection policy ensures Salder Consulting Ltd:

- Complies with data protection laws and follows good practice
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data protection law

New General Data Protection regulation (GDPR) (replacing the data protection act 1998), being enforced by ICO describes how organisations including Salder Consulting Ltd must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The GDPR regulation is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection.

People, risks and responsibilities

Policy scope

This policy applies to:

- The head office of Salder Consulting Ltd
- All staff of Salder Consulting Ltd
- All contractors, suppliers and other people working on behalf of Salder Consulting Ltd

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the GDPR Data Protection Regulation. This can include:

- Email, C.V Personal, Postal Address, date of birth, Psychometric data (like skills and knowledge, abilities, attitudes, personality traits, and educational achievement), point of view on assessment report showing if the person is fit for the Job, interview data. Any other personal information relating to individuals. NI number, Marital Status, next of Kin information, Passport Details, Bank Details, Telephone numbers, email address, other contact details of previous, potential and current employees C.Vs, Employment contracts or sub-contractors agreements if applicable.

Data protection risks

This policy helps to protect Salder Consulting Ltd from some very real data security risks, including:

- Breaches of confidentiality. For instance, information being given out inappropriately.
- Failing to offer choice. For instance, all individuals should be free to choose how the company uses data relating to them.
- Reputational damage. For instance, the company could suffer if hackers successfullygained access to sensitive data.

Responsibilities

Everyone who works for or with Salder Consulting Ltd has some responsibility for ensuring data is collected, stored and handled appropriately. Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The board of directors is ultimately responsible for ensuring that Salder Consulting Ltd meets its legal obligations.
- The Data Protection officer (Salder at dirk@salder-consulting.com) is responsible for:
  - Keeping the board updated about data protection responsibilities, risks and issues.
  - Managing Subject Access requests (SAR), which involves documenting and responding to all requests like transferring, acquiring and inquiring of personal information held by Salder Consulting Ltd, made by an individual or an organisation, relating to customers, contractors,

associates, partners and staff of Salder.

- Managing Subject Access Amendment requests (SAA), which involves documenting and responding to all requests made for changes and updates of personal information held by Salder Consulting Ltd, made by an individual or an organisation, relating to customers, contractors, associates, partners and staff of Salder.
- Validating fully all above requests before responding to them.
- Reviewing and updating all data protection procedures and related policies, in line with applicable regulations.
- Arranging data protection training and advice for the people covered by this policy.
- Handling data protection questions from staff and anyone else covered by this policy.
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

➡ **Alpha Tech (IT Services Provider)** is responsible for:

- Ensuring all systems, Computer - Printer and Cloud Based products used for storing data meet acceptable security standards and are fully supported.
- Technical and organisational security measures where appropriate, ensuring by regularly scanning systems using Webroot Anti-Virus and Computer monitoring of data, including data on local computer drives.
- Managing Disaster recovery plans, by taking measures such as Email Data backed up to cloud server for recovery.

General staff guidelines

➡ The only people able to access data covered by this policy should be those who need it for their work.

➡ Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.

➡ Salder Consulting Ltd will provide training to all employees to help them understand their responsibilities when handling data.

➡ Employees should keep all data secure, by taking sensible precautions and following the guidelines below.

➡ In particular, strong passwords must be used, and they should never be shared.

➡ Personal data should not be disclosed to unauthorised people, either within the company or externally.

➡ Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of after acquiring line managers approval.

➡ Employees should request help from company's data protection officer if they are unsure about any aspect of data protection.

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager or data protection officer. When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.
- Printouts data is kept in record, as long as necessary, i.e. when required by applicable law or by legitimate business reason, for example a- when there is a contract with Salder Consulting Ltd and for as long as it is required by law, after the contract is expired, or b- keeping psychometric data is only valid for 2 years and therefore deleted after that. We will review the data and ask for client's and employee's consent whether to keep, hold, transfer or remove the data, where necessary, for example, other than the Legal requirements mentioned above. Where we must archive the data, we will implement reasonable measures to protect the Personal Data and will only use if required for legitimate business purpose.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (like a CD or DVD or Memory Sticks), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers and should only be uploaded to an approved cloud computing service.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by approved security software and a firewall.
- Electronic data is kept in record, as long as necessary, i.e. when required by applicable law or by legitimate business reason, for example a- when there is a contract with Salder Consulting Ltd and for as long as it is required by law, after the contract is expired, or b- keeping psychometric data is only valid for 2 years and therefore deleted after that. We will review the

data and ask for client's and employee's consent whether to keep, hold, transfer or remove the data, where necessary, for example, other than the Legal requirements mentioned above. Where we must archive the data, we will implement reasonable measures to protect the Personal Data and will only use if required for legitimate business purpose.

Data use

Personal data is of no value to Salder Consulting Ltd unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally.
- Salder Consulting Ltd ensures that Data e.g. payslips are sent to the right recipient, whether sent electronically or by other means.
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data on the company secured server/computers.

Data accuracy

The law requires Salder Consulting Ltd to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort Salder Consulting Ltd should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.
- Salder Consulting Ltd will make it easy for data subjects to update the information Salder Consulting Ltd holds about them and ensures the authenticity of any requests made.
- Data should be updated as inaccuracies are discovered.

Subject access requests

All individuals who are the subject of personal data held by Salder Consulting Ltd are entitled to:

- Ask what information the company holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the company is meeting its data protection obligations.

If an individual contact the company requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to Salder Consulting Ltd. Requests can also be made via a standard request form, although individuals do not have to use this.

Salder Consulting Ltd will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing data for other reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Salder Consulting Ltd will disclose requested data however, will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

Providing information

Salder Consulting Ltd aims to ensure, through its Privacy Policy Document, that individuals are aware of their data being processed, they understand, how the data is being used, and how to exercise their rights.