Aspire Consulting and Training Ltd. Data Security, Protection and Privacy Policy

Version Number	4/01.01.2022
Issue Date (Last Review Date)	01/01/2022
Review Date	01/01/2023
Author and approved by	Jay Acharya (MD)

Jay Acharya

Aspire Consulting and Training Ltd.

Introduction

"The Company" and "We" relates to Aspire Consulting and Training Ltd.
This Data Protection Policy sets out the roles, responsibilities and procedures around the use of personal data within the Company.
This policy applies whenever you are collecting or handling personal data in any way.

Everyone has rights regarding the way in which their personal data is handled. During our activities we will collect, store and use personal data about clients, trainers, our associates and people in external organisations.

This policy applies to all employees, workers and contractors. Any breach of this policy may result in disciplinary action.

This policy does not form part of any employee's contract of employment, or any contract for the provision of services, and may be amended at any time.

Policy Scope

This policy applies to all employees, workers and contractors.
The aims of this policy are:
• To protect the rights, safety and welfare of individuals, in relation to the use of personal data.
• To help you understand the fundamentals of data protection law.
• To guide you to help ensure that we are compliant with data protection laws.
• To understand the risks to the Company (and specifically the company whom you are employed by and as set out in your employment contract ("**your Employer**")) of non- compliance with data protection laws.

Responsibilities
The Company is too small to employ a Data Protection Officer ("**DPO**") and therefore the Managing Director is responsible for overseeing compliance with the Data Protection Legislation and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Jay Acharya.

Definitions

What does the Law say?

What is the UK GDPR?

The General Data Protection Regulation ("GDPR") came into force on 25th May 2019 and became applicable to all EU Member States. In the UK, the UK GDPR is now in place to recognise the UKs exit from the European Union from 31st December 2020.

What is personal data?

Personal data is any data which relates to a living individual who can be identified from that data (or from that data and other information likely to come into your Employer's possession). It therefore captures a wide range of data. Examples of personal data are set out in **Schedule 1**. If you are unsure about whether certain information is personal data or not, please speak with the Data Protection Officer (please see paragraph 4 of this policy for more details).

What is sensitive personal data?

The Data Protection Laws class a certain type of personal data as sensitive personal data. A list of examples of sensitive personal data are set out in **Schedule 1**. It is important that you recognise what sensitive personal data is because the law imposes more stringent requirements around use of sensitive personal data and possibly means you need to get the consent of the individual about whose sensitive personal data you are using before you are lawfully permitted to use it.

Who regulates the GDPR in the UK?

In the UK, the Data Protection Laws are independently enforced by the Information Commissioner's Officer ("ICO").

What happens if we get it wrong?

The ICO has a wide range of powers. It can issue enforcement notices where it tells businesses to remedy a certain breach. It can also publicise data protection breaches on its website which could lead to negative publicity for the business in breach. It also has the right to audit your Employer and fine it up to €20 million or 4% of global turnover for breaches of the Data Protection Laws.

The 6 data protection principles

The GDPR sets out 6 data protection principles which you should be aiming to follow at all times. They are as follows:

1. **Fairly, lawful and transparent** – The first principle is that personal data shall be processed fairly, lawfully and transparently. The Data Protection Laws are not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the individuals whose data you are using. It also important to be transparent with individuals in relation to what you do with their data.

2. **Use it only for a limited purpose** – The second principle is that personal data shall be collected for specified, explicit and legitimate purposes and not processed in a manner incompatible with those purposes. As an employee, you may be involved in collecting personal data in different ways. This may include data you receive directly from individuals and data you receive from other sources. You must not use the data for your own personal purposes. Personal data which you collect in the course of your employment should be used strictly as part of your employment and only for the purpose for which it was collected.

3. **Data minimisation** – The third principle is that personal data shall be adequate, relevant and limited to what is necessary. You should only collect, use, access or analyse personal data to the extent that you need to.

4. **Accuracy** – The fourth principle is that personal data shall be accurate and, where necessary, up to date. You should check the accuracy of any personal data at the point of collection and at regular intervals afterwards. You should take all reasonable steps to destroy or amend inaccurate or out-of-date data.

5. **Data retention** – The fifth principle is that personal data shall be kept for no longer than is necessary. The Data Protection Laws do not tell us how long is necessary. We have therefore prepared a separate Data Protection Retention Policy to guide you in determining how long to keep certain types of information. Please refer to that policy for further details about how long you should be keeping certain types of personal data and how you should be deleting personal data. It is

important that you follow the Personal Data Retention Policy and it should be read in conjunction with this policy.

6. The security (or "ATOM") principle – The sixth principle is that personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful use of personal data and against accidental loss, destruction or damage. The GDPR says that we must use "appropriate, technical and organisational measures" (try using the acronym "ATOM" to help you remember) to keep data secure. Security of personal data applies to a range of areas, including IT security, and it particularly should be applied throughout your day-to-day activities. You should review the Company's IT policies for further details about using IT securely.

There are additional principles that we believe are just as important as those set out above and these are set out below.

Respecting the individual's legal rights

Your Employer will also be required to process personal data in accordance with the rights of data subjects (i.e. the individuals about you're your Employer holds personal data). Please see paragraphs 9 and 10 for further detail about individuals' right of access to the information your Employer holds about them (commonly known as a subject access request or "SAR") and their right for information about them to be erased (typically referred to as the right to be forgotten).

Don't let personal data leave the UK without telling us

Personal data must not leave the European Economic Area unless certain legal protections are in place. If you would like further details about this principle or have any queries, please speak to the Data Protection Officer (please paragraph 4 below). If you are aware of personal data being transmitted outside of the UK, you need to tell the Data Protection Officer immediately. This might mean having to do some investigation as to how personal data flows in and out of the organisation.

Accountability

We will all need to take responsibility for the principles above and be able to demonstrate that we are complying with them. Please make sure that you are able

to show the Data Protection Officer how you are complying with this policy and the Personal Data Retention Policy.

Process

Taking Ownership

The GDPR introduces a new concept called data protection by "**design and default**". It essentially means that we all have a responsibility to proactively build the principles, as detailed above, into our everyday activities. Don't be afraid to question current or old practices or technology if you think they do not follow good data protection practice and raise any issues or concerns with the Data Protection Officer.

New Ideas

You may want to introduce something new and innovative to either your Employer or the wider Group. It could be a new piece of technology, or you may be looking to introduce a campaign which involves the use, in some way, of personal data. Or you might want to implement a new piece of software.

It is important that, before implementing anything new involving or impacting upon personal data, you speak with the Data Protection Officer. Under the new GDPR concept of data protection by design and default, we will need to ensure that we have built good data protection practice into any new idea before implementing the idea. Sometimes, this will require a formal data privacy impact assessment (with which the Data Protection Officer will provide assistance) where the new idea is potentially high risk to the privacy of members of staff.

Data Breaches

A personal data security breach is any security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. It could be because of a cybercrime. Or it could be that you, or someone you know, have accidentally shared personal data with another organisation or person without permission.

If you become aware of a personal data security breach you must inform the Data Protection Officer immediately, providing as much background detail as possible.

This is because the GDPR requires your Employer to report personal data breaches to the regulator within 72 hours of first becoming aware of it. **Please do not report the breach to the ICO yourself.**

Sharing Information with Other Organisations

If you are looking at engaging with any new supplier, and you know that the supplier will be obtaining personal data relating to members of staff or other groups of people, you will need to contact the Data Protection Officer as soon as possible before engaging with that supplier.

The GDPR requires your Employer to (a) vet these suppliers to ensure that they offer an appropriate level of security of personal data and (b) make sure that there is a written contract between the supplier and your Employer and that it is GDPR-compliant before being signed.

Dealing with Subject Access Requests

A subject access request ("**SAR**") is a written request from an individual to obtain information their Employer holds about him or her. This is a statutory right, however it is not without its complications and it doesn't just mean disclosing every piece of information because there might be legal reasons to withhold certain information. The individual issuing a SAR could be a client, third-party trainer, member of staff or member of the public. Not everyone who requests personal data will be entitled to receive it, therefore, it is important we verify an individual's right to receive personal data, particularly where the personal data is not about themselves.

As there are strict time periods for complying with a SAR (1 calendar month from the date of the SAR), it is important that you **immediately** notify the Data Protection Officer who will then assist with the request accordingly.

Please do not respond to the individual without first consulting with the Data Protection Officer.

Right To Be Forgotten Requests

A right to be forgotten request is a written request from an individual to erase information a company holds about him or her. Like SARs, this is a statutory right but not as straightforward as you might think and it doesn't just mean deleting every piece of information about the individual because there might be legal

reasons to keep certain information. As with SARs, please make sure that you contact the Data Protection Officer **immediately** before responding to the individual making the request. **Please do not respond to the individual without first consulting with the Data Protection Officer.**

Schedule 1

Example of Personal Data

Personal Data	Sensitive Personal Data
Name (first name or second name)	Religious expression
Age	Physical or mental condition
Address	Political views and beliefs
Phone Number	Racial or ethnic origin
Email Address	Criminal record checks
Photograph	Trade union membership
Location	Sex life
Opinion	Sexual orientation
Bank Details	Biometric data (e.g. data obtained from fingerprint or retina scanning)
Salary	
Staff training records	
Letters	
Contracts	

Please note that these are not exhaustive lists.