DATA PROTECTION POLICY

www.invenio-solutions.com

DOCUMENT CONTROL

DOCUMENT NAME	Data Protection Policy
ABSTRACT	This document details the data protection policy & guidelines for the management and employees
DOCUMENT REFERENCE	HRD005

AUTHORISATION

Process Owner	**Reviewed By**	**Authorised By**
Name : Bipin Pendyala	Name : Naveen Agarwal, Steve Coxhead	Name : Arun Bala
Signature:	Signature :	Signature :

SECURITY CLASSIFICATION: Company Confidential

DISTRIBUTION LIST

Master HRD Department
Copies Electronic only

VERSION HISTORY

VERSION	DATE	PREPARED BY	CHANGES & REASONS FOR CHANGE
Draft 1.0	15/05/2019	Bipin P	
Issue 1.0	21/06/2019	Bipin P	

TABLE OF CONTENTS

1. PURPOSE AND SCOPE

Invenio Business Solutions Limited (the "Company") collects and processes personal data relating to our current, past and prospective workforce. The Company may also collect and process a range of personal data relating to its customers, clients, suppliers and other business contacts. Company recognises the need to treat that information in an appropriate and lawful manner and are committed to protecting the privacy and security of individuals' personal data.

This policy summarises and sets out how the Company handles personal data and complies with our data protection obligations. All staff must read, understand and comply with this policy and any related policies, operating procedures or processes, privacy notices and attend any required training on its requirements.

Our board have overall responsibility for the effective operation of this policy and for ensuring that the Company implements appropriate practices, processes, controls and trains to ensure such compliance. All staff operating at management level have a responsibility to set an appropriate standard of behaviour and to lead by example. They should ensure those they manage adhere to this policy and receive appropriate training to ensure such compliance. The Company has appointed Naveen Agarwal, CTO as the person with responsibility for overseeing this policy. Questions about this policy, or requests for further information, should be directed to him in the first instance.

2. DEFINITIONS

The following definitions are used throughout this policy:

"Personal data" is any information that relates to a living individual who can be identified from that data (or from that data and other information in our possession). It accordingly excludes anonymous data. Personal data can be factual or it can be an opinion.

"Processing" is any activity that involves use of personal data whether or not by automated means, including collecting, storing, amending, disclosing or destroying it.

"Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health, sex life or sexual orientation, genetic data and biometric data.

"Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

.

3. DATA PROTECTION PRINCIPLES

When processing personal data the Company, and employee, must comply with the following data protection principles:

- personal data must be processed lawfully, fairly and in a transparent manner;
- personal data must only be processed for specified, explicit and legitimate purposes and will not further process that data in a manner incompatible with those purposes;
- personal data processed by the Company will be adequate, relevant and limited to what is necessary for the purposes for which it is processed;
- personal data must be accurate and, where necessary, is kept up to date and all reasonable steps are taken to ensure that inaccurate personal data is rectified or deleted without delay;
- personal data is not kept in a form which permits identification of the individual for any longer than is necessary for the purposes for which it is processed; and
- personal data is processed in a manner that ensures appropriate security of the data. It adopts appropriate measures to make sure that personal data is protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

The Company provides privacy notices to relevant individuals informing them about their rights, how it complies with its data protection obligations, how it collects and uses personal data, the reasons for processing personal data and the legal basis for any such processing. Such information may also be included in its contractual documents with third parties.

The Company must only use personal information for the purposes for which it was collected, unless it reasonably considers that it needs to use it for another reason and that reason is compatible with the original purpose. If the Company needs to use personal information for an unrelated purpose, it must notify the relevant individuals and explain the legal basis which allows it to do so.

The Company must maintain appropriate records of the processing activities for which it is responsible in accordance with the requirements of the General Data Protection Regulation (GDPR).

The Company will provide appropriate training to all staff about their data protection responsibilities. The level of training will reflect their role's access to personal data and responsibility for implementing this policy.

4. DATA SECURITY

The Company has appropriate technical and organisational measures and safeguards in place to prevent unauthorised or unlawful processing, to prevent personal data from being lost, accidentally destroyed, misused or disclosed, and to ensure that it is not accessed except by the Company's employees and other staff when necessary in the proper performance of their duties. Company will regularly evaluate and test the effectiveness of these measures and safeguards. Further details about the Company's security procedures can be requested from Naveen Agarwal, CTO and include, for example, having systems that allow the Company to create and improve security features, restricting access, regular audits and testing of these processes and the integrity and resilience of processing systems and services.

Employees must comply with the Company's procedures and processes to ensure data security and also not act in a manner which may invalidate or render ineffective the Company's measures and safeguards

5. THIRD PARTIES

Where the Company engages third parties to process personal data on its behalf, the Company must ensure the third party provides adequate guarantees in terms of data security standards, policies, procedures, security measures in place, reliability and resources to implement appropriate technical and organisational measures to ensure personal data is processed in accordance with both companies' data protection obligations.

The Company must have in place a contract or other legal arrangement with the third party setting out the type of personal data that will be processed, the duration of the processing, the nature and purposes of the processing, the categories of data subjects, the obligations and rights of the Company, the specific tasks and responsibilities of the third party and the requirements around returning or deleting the personal data after completion of the contract.

6. INTERNATIONAL DATA TRANSFERS

The GDPR restricts data transfers to countries outside the European Economic Area (EEA) in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. One transfers Personal Data originating in one country across borders when one transmits, sends, views or accesses that data in or to a different country.

The Company may only transfer Personal Data outside the EEA in limited and necessary circumstances.

The Company envisages transferring personal data to India outside the EEA and to ensure that personal information receives the adequate level of protection the data is transferred on the basis of the model clauses approved by the European Commission.

7. IMPACT ASSESSMENTS

When appropriate, including where processing is likely to result in a high risk to an individual's rights and freedoms and in the event of all major system or business change programs involving the processing of personal data, the Company will carry out a data protection impact assessment to determine the necessity and proportionality of processing. This will include a description of the processing, its purposes, the Company's legitimate interests if appropriate, an assessment of the risks for individuals and the measures put in place to mitigate those risks. Where the impact assessment indicates the processing involves a high risk that cannot be mitigated by appropriate measures in terms of available technology and costs of implementation company shall consult the supervisory authority prior to the processing.

8. DATA BREACHES

If the Company discovers that there has been a personal data breach that poses a risk to the rights and freedoms of individuals, company shall report it to the Information Commissioner's Office without undue delay and, where feasible, within 72 hours of discovery. This will include any act or omission that compromises the security, confidentiality, integrity or availability of personal data or the safeguards that the Company or a third party has put in place to protect it that poses a risk to the rights and freedoms of individuals. The Company will record all data breaches.

Where appropriate and if the breach is likely to result in a high risk to the rights and freedoms of individuals, company will tell affected individuals without undue delay that there has been a breach and provide them with information about its likely consequences and the mitigation measures company has taken.

Please note that it is crucial that employees notify Naveen Agarwal, CTO as soon as they become aware of any potential data breach, regardless of how serious he/she believe that breach to be. Employees should preserve all evidence relating to the potential personal data breach.

9. DATA SUBJECTS' RIGHTS

Individuals have a number of rights in relation to their personal data. They have the right to:

- access and obtain a copy of the personal data company holds about them on request (also known as a subject access request);
- require the Company to correct inaccurate or incomplete personal data;
- require the Company to delete or stop processing their personal data where there is no good reason for the Company continuing to process it or where they have exercised their right to object to processing (see below);
- object to the processing of their personal data where the Company is relying on its legitimate interests (or those of a third party) as the legal ground for processing; and
- request the restriction of processing of their personal data. This enables them to ask the Company to suspend the processing of their personal data, for example if they want the Company to establish its accuracy or the reason for processing it.

To ask the Company to take any of these steps, the individual should send the request to Naveen Agarwal, CTO at Naveen.agarwal@invenio-solutions.com. If an employee receives any such request, or indeed any request for personal data, this should be referred to Naveen Agarwal immediately.

In some cases, the Company may need to ask for proof of identification and/or require the individual to specify the information or processing activities to which the request relates before a request can be processed. Employee should not personally respond to any such request for information and any communications should be sent or approved by Naveen Agarwal.

The Company will normally respond to a request within one month from the date the request is received. However, in some cases, such as where the Company processes large amounts of the individual's personal data, it may respond within three months of the date the request is received. The Company will write to the individual within one month of receiving the original request to tell him/her if this is the case.

If the Company receives a subject access request it will provide the individual with a copy of the personal data requested. This will normally be in electronic form if the individual has made a request electronically, unless he/she agrees otherwise. If the individual wants additional copies, the Company may charge a reasonable fee.

If a subject access request is manifestly unfounded or excessive, the Company is not obliged to comply with it. An individual will not normally have to pay a fee to access their personal information or to exercise any of the other rights listed above. However, the Company may charge a reasonable fee if a subject access request is clearly unfounded or excessive. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the Company has already responded. If an individual submits a request that is unfounded or excessive, the Company will notify him/her that this is the case and whether or not it will respond to it.

The Company will update personal data promptly if an individual advises that his/her information has changed or is inaccurate. If company receives any information about changes to an individual's personal data, including any change of name, address or other personal details, company shall ensure that such request is verified as genuine and then actioned.

If an individual believes that the Company has not complied with their data protection rights, they have the right to complain at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

10. OBLIGATIONS ON STAFF

When working for or on behalf of the Company all staff must:

- comply with the Company's commitments set out in this policy when processing personal data;
- promptly attend training sessions regarding data protection and data security as requested by the Company and ensure any team members for which employee have management responsibility have attended appropriate training dependent on their role;
- process personal data on a need to know basis and for authorised and lawful purposes in accordance with the relevant privacy notices only;
- ensure that prior to transferring data to a third party or outside the European Economic Area there are adequate security measures in place in compliance with the relevant restrictions set out in this policy;
- ensure that when personal data is no longer needed for specified purposes it is deleted or anonymised in accordance with the Company's the data retention guidelines set out in the relevant privacy notice;

- comply with obligations of confidentiality and the Company's information security measures, policies and procedures as put in place from time to time, including those relating to data security, password protection and encryption, use of and access to the Company's IT and communications systems, access to premises, use of personal devices for work purposes and use of removable storage devices;
- notify Naveen Agarwal, CTO immediately in the event he/she become aware of or suspect there has been a personal data breach; and
- notify Naveen Agarwal, CTO immediately in the event he/she receive a request from an individual exercising their data subjects' rights detailed above. Individual must not disclose personal data requested without having first verified that person's identity.

All staff are responsible for helping the Company keep their own personal data up to date. Employees should let the Company know if personal data provided earlier changes, for example if employee moves to a new house or changes bank account details.

11. BREACHES OF THIS POLICY

All staff must comply with this policy and any breaches will be taken very seriously.

Any breaches by an employee are likely to be treated as gross misconduct and result in action being taken under the Company's Disciplinary Procedure up to and including summary dismissal.

If any other (non-employee) member of staff fails to comply with this policy the Company may decide to stop providing that member of staff with work or terminate their contract with the Company immediately and without notice or compensation.