HI-WAY SERVICES LTD

GENERAL DATA PROTECTION REGULATION (GDPR) POLICY

New data protection legislation is due to come into force in May 2018, which aims to protect the privacy of all EU citizens and prevent data breaches. It will apply to any public or private organisation processing personal data. Established key principles of data privacy remain relevant in the new Data Protection Legislation but there are also a number of changes that will affect commercial arrangements, both new and existing, with suppliers.

The Data Protection Legislation comprises: i) the General Data Protection Regulation (GDPR) which comes into force on 25 May 2018; and ii) the Data Protection Act (DPA) 2018 which is anticipated to come into force (subject to Parliamentary approval) on 6 May 2018 for law enforcement processing, and 25 May for GDPR.

STANDARD DEFINITIONS

Law: means any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the Provider is bound to comply;

Provider Personnel (the Company): means all directors, officers, employees, agents, consultants and contractors of the company and/or of any Sub-Contractor engaged in the performance of its obligations under these regulations.

GDPR CLAUSE DEFINITIONS:

Data Protection Legislation:
(i) the GDPR, any applicable national
implementing Laws as amended from time to time
(ii) the DPA 2018 to the extent that it relates to the processing of personal data and privacy;
(iiii) all applicable Law
about the processing of personal data and privacy;

Data Protection Impact Assessment: an assessment by the Data Controller of the impact of the envisaged processing on the protection of Personal Data;

Data Loss Event: any event that results, or may result, in unauthorised access to Personal Data held by the company under this Agreement, and/or actual or potential loss and/or destruction of Personal Data including any Personal Data

DPA 2018: Data Protection Act 2018;

GDPR: the General Data Protection Regulation (Regulation (EU) 2016/679);

LED: Law Enforcement Directive (Directive (EU) 2016/680).

Protective Measures: appropriate technical and organisational measures, which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such systems.

Sub-processor: any third Party appointed to process Personal Data on behalf of the Company.

Key points

- The General Data Protection Regulation comes into force on 25 May 2018.
- Employees/Workers have a legal right to access information that an employer may hold on them.
- The Data Protection Act contains 8 principles that everyone responsible for using data has to follow.
- All company employees have a responsibility under the act to ensure that their activities comply with the Data Protection.
- Data Protection applies when monitoring employee's telephone calls, emails and CCTV.
- Employees who feel the organisation has misused information or hasn't kept it secure can contact the Information Commissioner's Office.

The European Union's GDPR (General Data Protection Regulation) comes into force in the UK on 25th May 2018. The GDPR will bring in stricter obligations that all employers must follow.
The ICO (Information Commissioner's Office) has published an overview of the regulation and has a checklist of 12 steps you can take to get ready.
For more information, go to the **ICO website**.

Until May 25 2018, The Data Protection Act 1998 still applies. The Data Protection Act is concerned with respecting the rights of individuals when processing their personal information.
This can be achieved by being open and honest with employees about the use of information about them and by following good data handling procedures.
The act is mandatory and all organisations that hold or process personal data must comply.

The Data Protection Act contains 8 principles and these will be upheld within the GDPR:

- personal data should be processed fairly and lawfully
- data should be obtained only for one or more specified and lawful purposes
- the data should be adequate, relevant and not excessive
- it should be accurate and where necessary kept up to date
- any data should not be kept for longer than necessary
- personal data should be processed in accordance with the individuals rights under the Data Protection Act
- data should be kept secure
- personal data should not be transferred outside the European Economic Areas unless the country offers adequate data protection.

All employees have a responsibility under the Act to ensure that their activities comply with the Data Protection Principles.
Directors/Line managers/Supervisors have responsibility for the type of personal data they collect and how they use it.
Employees should not disclose personal data outside the company's procedures, or use personal data held on others for their own purposes.

Employees/Workers have a legal right to access information that an employer may hold on them. This could include information regarding any grievances or disciplinary action, or information obtained through monitoring processes.
Arrangements should be in place to deal with requests as a 40-day time limit is stipulated.
Information can be withheld if releasing it would make it more difficult to detect crime or the information is about national security.
If an employee feels the organisation has misused information or hasn't kept it secure they can contact the Information Commissioner's Office.

Monitoring employees - CCTV, telephone calls, emails
The Data Protection Act will apply if employers are monitoring employees; for example to detect crime or excessive private use of e-mails, internet use etc.
However, the act requires that employees/workers should be aware of the nature and reason for any monitoring.

Health Information
Employers can seek to collect information regarding an employee's health if the employee freely gives consent.
Employers should consider why they need the information and exactly what information is needed. This information once collected should be held securely, this could be allowing only one or two people access to the information or by password protecting it.
Employers should check that the information collected could be justified.

The following are steps that the company will undertake to ensure compliance with GDPR.

The Company will ensure that decision makers and key people in the company are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have and identify areas that could cause compliance problems under the GDPR.

The company will ensure that a risk register is compiled for this purpose.

The company will establish and understand what information, documentation and personal data it holds, where it came from and who the company share's it with.

The company will organise an information audit across the organisation or within particular business areas.

The GDPR requires that the company maintain records of its processing activities. It will update rights for a networked world. If the company holds inaccurate personal data and the company has shared this with another organisation, the company will inform the other company/organisation about the inaccuracy so it can correct its own records.

The company will compile information about what personal data it holds, where it came from and who the company share it with. This will help the company to comply with the GDPR's accountability principle, which requires companies/organisations to be able to show how they comply with the data protection principles, for example by having effective policies and procedures in place.

The company will review its current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

At the present time when the company collects personal data, it provides certain information, such as the individual's identity and how the company intends to use this information. This is usually done through a privacy notice. Under the GDPR there are some additional things you will have to tell people. For example, you will need to explain your lawful basis for processing the data, your data retention periods and that employees/workers have a right to know and access.

The GDPR requires the information to be provided in concise, easy to understand and clear language.

The company will check its procedures to ensure that they cover all the rights individuals have, including how it will delete personal data or provide data electronically and in a commonly used format.

The GDPR includes the following rights for individuals:

- the right to be informed of access
- the right to rectification;
- the right to erasure
- the right to restrict processing
- the right to data portability
- the right to object
- the right not to be subject to automated decision-making including profiling
- the right to take account of the new rules

On the whole, the rights individuals will enjoy under the GDPR are the same as those under the DPA but with some significant enhancements. The company will check its procedures and will implement a system if someone asks to have their personal data deleted.

The company will consider if the systems will help locate and delete the data? The company will decide and acknowledge who will make the decisions about deletion?

The right to data portability is new. It only applies:

- to personal data an individual has provided to a data controller;
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means.

The company will consider whether it needs to revise its procedures and make any changes. The company will provide the personal data in a structured commonly used and machine-readable form and provide the information free of charge.

The company will update its procedures and plan how and who will handle requests

- In most cases you will not be able to charge for complying with a request.
- You will have a month to comply, rather than the current 40 days.
- You can refuse or charge for requests that are manifestly unfounded or excessive.
- If you refuse a request, you must tell the individual why and that they have the right to complain to the supervisory authority and to a judicial remedy. You must do this without undue delay and at the latest, within one month.

The company will identify the lawful basis for its processing activity in the GDPR, document it and update its privacy notice to explain it.

Under the GDPR some individuals' rights will be modified depending on the company's lawful basis for processing their personal data. The most obvious example is that individuals will have a stronger right to have their data deleted where the company use consent as its lawful basis for processing.

The lawful bases in the GDPR are broadly the same as the conditions for processing in the DPA. The company will review the types of processing activities it undertakes and will identify its lawful basis for doing so. The company will document its lawful bases in order to comply with the GDPR's 'accountability' requirements.

The company will review how it seeks, records and manages consent and whether it needs existing consents now if they don't meet the GDPR standard.

Consent must be freely given, specific, informed and unambiguous. There must be a positive opt-in – consent cannot be inferred from silence, pre- ticked boxes or inactivity. It must also be separate from other terms and conditions, and the company will need to have simple ways for people to withdraw their consent. The company will take particular care and ensure that consent has been verifiable, it is understood generally that individuals have more rights where the company relies on consent to process their data.

The company will ensure that if it relies on individuals' consent to process their data, the company will make sure it meets the GDPR standard on being specific, granular, clear, prominent, opt-in, properly documented and easily withdrawn.

The company will ensure that it has the right procedures in place to detect, report and investigate a personal data breach.

The GDPR introduces a duty on all companies/organisations to report certain types of data breach to the ICO, and in some cases, to individuals. The company will notify the ICO of a breach where it is likely to result in a risk to the rights and freedoms of individuals – if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

If the company establishes that a breach is likely to result in a high risk to the rights and freedoms of an individual, it will also notify those concerned directly in most cases.

The company will put into place procedures to effectively detect, report and investigate a personal data breach. The company will conduct an internal audit to assess the types of personal data it holds and document where it would be required to notify the ICO or affected individuals if a breach occurred.

Failure on the part of the company to report a breach when required to do so could result in a fine, as well as a fine for the breach itself.

It has always been good practice to adopt a privacy by design approach and to carry out a Privacy Impact Assessment (PIA) as part of this. However, the GDPR makes privacy by design an express legal requirement, under the term 'data protection by design and by default'. It also makes PIAs – referred to as 'Data Protection Impact Assessments' or DPIAs – mandatory in certain circumstances.

Data Protection by Design and Data Protection Impact

A DPIA is required in situations where data processing is likely to result in high risk to individuals, for example:

- where a new technology is being deployed;
- where a profiling operation is likely to significantly affect individuals; or
- where there is processing on a large scale of the special categories of data.

If the company considers that the DPIA indicates that the data processing is high risk, and it cannot sufficiently address those risks, the company will consult the ICO to seek its opinion as to whether its processing operation complies with the GDPR.

The company will designate someone to take responsibility for data protection compliance and assess where this role sits within the company's structure and governance arrangements.

The company will ensure either that someone in the organisation, or an external data protection advisor, takes proper responsibility for its data protection compliance and has the knowledge, support and authority to carry out their role effectively.

Signed: 

Andy O'Reilly Managing Director

Date 08/01/20