Scope HR Solutions Limited

GDPR "General Data Protection Regulation"

And Privacy Policy

Version: 1.1

Date: 12/05/2018

Author: P. Baker – Commercial Director/Data Controller

Next Review Date: 12/11/2018

1. Introduction

On the 25th May 2018 the "General Data Protection Regulation 2016" becomes Law replacing the EU Data Protection Directive of 1995 and supersedes the Laws of individual Member States that were developed in compliance with the Data Protection Directive 95/46/EC the purpose is to protect the "rights and freedoms" of living individuals and to ensure that personal data is not processed without their knowledge and it is processed with their consent.

As a Business Scope HR Solutions is all about Individuals, so it is safe to say this is one of the most significant pieces of legislation that impacts on every process within the organisation, Individuals support, protection and welfare are at the centre of the Business core values.

At this point it is essential to understand that while this document replaces the current Scope HR Solutions Data Protection Policy, because of the business ethics and values we are fortunate in that we are not "reinventing the wheel" but enhancing an already "robust system".

GDPR has several, principles that underpin the legislation and are outlined using the following terms (These are not to be confused with the defined rights of the Data Subject):

1. Lawfulness, fairness and transparency – keep it legal and fair; say what you are going to do with the data in clear terms.
2. Purpose limitation – do not do more with the data than you said you would.
3. Data minimisation – do not collect more data than you need.
4. Accuracy – keep it up to date and deal with inaccuracies as soon as possible; check and verify.
5. Storage limitation – do not keep the data for longer than necessary.
6. Integrity and confidentiality – keep the data safe while you have it.
7. Accountability – be able to demonstrate compliance.

If as an Individual the above principles and subsequent contents of this document are not fully implemented and adhered to via robust processes within the business and the Directors, Data Controller or the Compliance and Data Protection Officer have not been able to address these concerns we would encourage you to make an official complaint to the Information Commissioners Office (ICO).

2. Definitions

Listed are both internal definitions for clarity and those defined that are applicable to Scope HR Solutions within Article 4 EU GDPR

Directors – Those responsible for the overall business performance and strategy in relation to data handling.

Data Controller – The individual responsible for deciding what data is collected and how it is used in line with GDPR legislation supported by a fully Auditable trail.

Compliance and Data Protection Officer – the individual responsible for implementing SOP's, RA's(Data Protection Impact Assessment) based on identified CCP's, ensuring engagement, support and mentoring of Colleagues. monitoring internal performance on an ongoing basis combined with a commitment to an Audit program supported by CA's to deliver 100% Compliance.

Colleague – an individual employed by Scope HR Solutions who processes personal data in line with the business strategy and under the direction of the data controller within the framework of the processes that have been mapped and agreed

SOP's – Standard Operating Procedures to demonstrate in flow diagram format the mapping of the required process to achieve GDPR Compliance.

CCP's – Critical Control Points that through the mapping process have been identified as areas of high risk to GDPR Compliance.

CP's – Control Points that through the mapping process have been identified as points of interaction and low risk are required to be reviewed during Audit process.

GDPR – General Data Protection Regulation

ICO – Information Commissioners Office based at Wycliffe House, Water Lane, Wilmslow, SK9 5AF helpline contact number 0303 123 1113 Main aim is to ensure Compliance with GDPR legislation to improve the information rights practises of organisations. Any concern should be raised within 3 months of last contact with the organisation or individual.

Individual – refers to any candidate prospective or during the process of recruitment, registration and induction prior to initial assignment thereafter Associate. Natural person or data subject.

Personal Data – means any information relating to an identified or identifiable Individual (Data Subject) by reference to an identifier such as a name, payroll number or any other reference number, address, email or any media account and to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of an Individual.

Processing – means any process or set of processes that is performed on personal data or sets of personal data whether or not by automated means such as collection, recording, organisation, structuring, storage, adaptation (changing), retrieval, consultation, use,

disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Restriction of processing - means the marking of stored personal data with the aim of limiting their processing in the future requested by the Individual.

Profiling – means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an Individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Pseudonymisation – means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific Individual without the use of additional information, provided such information is kept separately and is subject to technical or organisational measures to ensure that the personal data is not attributed to an Individual.

Filing system – means any structured set of personal data which is accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

Processor – means a colleague who processes data in the framework of organisational processes.

Recipient – means an Individual, public authority, agency or another body to which the personal data is disclosed. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with law shall not be regarded as a recipient; the processing of that data by public authorities shall be in compliance with the applicable data protection legislation according to the purposes of the processing.

Third party – means anybody, legal, agency or public other than the Individual, data controller, processor and persons who, under the direct authority of the controller are authorised to process personal data.

Consent – of the Individual means any freely given, specific, informed and unambiguous indication of the Individuals wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Personal data breach – means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Relevant and reasoned objection – means an objection to a draft decision as to whether there is an infringement of GDPR or whether envisaged action in relation to the controller or processor complies with this regulation, which clearly demonstrates the significance of the risks posed by the draft decision about the fundamental rights and freedoms of the individual.

3. The “Individual”

This Policy protects the rights and freedoms of the Individual based on GDPR legislation, in this respect a Colleague becomes an Individual in relation to their personal data and in every respect the policy would apply.

4. The GDPR Defined Rights of the Individual

The Individual has very clearly defined rights within the GDPR legislation, Scope HR Solutions want to ensure every Individual is fully aware of their rights and the action they are able to take in the event of a breach, to ensure this is the case the “GDPR Advice Note” has been issued and is displayed at All Scope HR Solutions locations and a hard copy is handed to each Individual (in their native Language) during the registration process which is done prior to any personal data being collected. Each of these rights are supported by appropriate procedures within Scope HR Solutions that allow the required action to be taken within the timescales stated in the GDPR, these are listed below alongside the rights of the Individual:

1. The right to be informed – When data is collected (if supplied by the individual) or within 1 month (if not supplied by the Individual).
2. The right of access – 1 month
3. The right of rectification – 1 month
4. The right to erasure – without undue delay
5. The right to restrict processing – without undue delay
6. The right to data portability – 1 month
7. The right to object – On receipt of objection
8. Rights in relation to automated decision making and profiling

While these are the timescales stated within the GDPR, Scope HR Solutions are committed to achieving reduced timescales and without undue delay is 24 hours from point of notification.

5. Lawfulness of Processing

There are 6 alternative ways in which the lawfulness of a specific case of processing personal data may be established under GDPR. It is Scope HR Solutions policy to identify the appropriate basis for processing and to document it, in accordance with the regulation. The options are described as follows:

1. Consent

Unless it is necessary for a reason allowable in the GDPR, Scope HR Solutions will always obtain explicit consent from an Individual to collect and process their data. Transparent information about our usage of their personal data will be provided to the Individual at the time consent is obtained and their rights to their data explained.

If the personal data is not obtained directly from the Individual, then this data will be provided to the Individual at the earliest opportunity after the data is received and in any event within 1 month. Achieving consent has been rationalised due to the diversity and usage of the personal data within Scope HR Solutions to ensure the obligations to the Individual's rights and freedoms are met under GDPR.

2. **Performance of a Contract**

Where the personal data collected and processed from the individual is required to fulfil a contract, explicit consent is not required. This will often be the case where the contract cannot be completed without the personal data in question e.g. PPE cannot be delivered without an address.

3. **Legal Obligation**

If the personal data is required to be collected and processed to comply with the Law, then explicit consent is not required. This is the case for example to data related to taxation.

4. **Vital Interests of the Individual**

In a case where the personal data is required to protect the vital interests of an Individual or of another Individual, then this may be used as the lawful basis for processing. Scope HR Solutions will retain reasonable, documented evidence that this is the case, whenever this reason is used as the lawful basis of the processing of personal data.

5. **Task Carried Out in the Public Interest**

Where scope HR Solutions needs to perform a task that it believes is in the Public Interest or as part of an Official Duty then the Individuals consent will not be requested. The assessment of the public interest or official duty will be documented and made available as evidence where required.

6. **Legitimate Interests**

If the processing of specific personal data is in the legitimate interests of Scope HR Solutions and is judged not to affect the rights and freedoms of the Individual in a significant way, then this may be defined as the lawful reason for the processing. Again, the reasoning behind this view will be documented.

6. Privacy by Design

Scope HR Solutions has adopted the principle of privacy by design and will ensure that the definition and planning of all new or significantly changed processes and systems that collect personal data will be subject to due consideration of privacy issues, including RA (Data Protection Impact Assessments), SOP's, CCP's and CP's.

The RA will include:

- Consideration of how personal data will be processed and for what purpose

- Assessment of whether the proposed processing of personal data is both necessary and proportionate to the purpose
- Assessment of the risks to individuals in processing the personal data
- What controls (CCP's and CP's) to address the risks and demonstrate Compliance

Use of techniques such as data minimisation and pseudonymisation will be considered where applicable and appropriate.

7. Contracts Involving the Processing of Personal Data

Scope HR Solutions will ensure that all relationships it enters into that involve the processing of personal data are subject to a documented contract.

They will contain the specific information and terms of the GDPR legislation and that the controller must specify a set of minimum terms within the contract related to data protection as follows:

- processes the personal data only on documented instructions from the controller
- ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality
- takes all measures required pursuant to Article 32 of the GDPR
- respects the conditions referred to in paragraphs 2 and 4 of Article 28 of the GDPR for engaging another processor
- assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the Individual's rights
- assists the controller in ensuring compliance with the obligations pursuant to Article 32 to 36 of the GDPR
- at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless by law storage of the personal data is required
- makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller

8. Security

Article 32 – Security of processing requires both controllers and processors to "implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk"

Scope HR Solutions as a business, the ability for unlawful access to IT systems has been minimised by all implemented processes being investigated, reviewed and updated where required to ensure they are GDPR compliant. Colleagues have been briefed, engaged and trained as to the impact of potential exposure to any third party (this also applies to any unauthorised Colleague) of personal data without the appropriate consent and how to guard the Individual from exposure. SOP's are to be followed with CCP's and CP's monitored to ensure protection against breach. In the event of a breach of any system whether Manual or Technical the Data Controller will immediately be advised in order that the breach can be assessed and the appropriate CA (Corrective Action) can be taken.

9. International Transfers of Personal Data

If at any point Scope HR Solutions has a request or are required to transfer personal data outside of the EU it will be carefully reviewed prior to the transfer taking place to ensure it falls within the limits imposed by the GDPR. This depends partly on the European Commission's judgement as to the adequacy of the safeguards for personal data applicable to the receiving country and this may change over time.

10. Data Protection Officer

A defined role of Data Protection Officer is required under GDPR if an organisation is a public authority, if it performs large scale monitoring or if it processes particularly sensitive types of personal data on a large scale. The Data Protection Officer is required to have an appropriate level of knowledge and can either be an in-house resource or outsourced to an appropriate service provider.

Based on these criteria Scope HR Solutions have appointed a Compliance and Data Protection Officer.

11. Breach Notification

It is Scope HR Solutions policy to be fair and proportionate when considering the actions to be taken to inform affected parties regarding breaches of personal data. In line with the GDPR, where a breach is known to have occurred which is likely to result in a risk to the rights and freedoms of individuals the office of the ICO will be informed as soon as practicably possible but in any event no longer that 72 hours of the incident.

12. Summary (Addressing Compliance to the GDPR)

The following actions are undertaken to ensure that Scope HR Solutions complies at all times with the accountability principle of the GDPR:

- The legal basis for processing personal data is clear and unambiguous
- The Compliance and Data Protection Officer is appointed with specific responsibility for data protection in the organisation
- All colleagues involved in handling personal data understand their responsibilities for following good data protection practice
- Training in data protection has been provided to all colleagues
- Processes and systems regarding consent are followed
- Through transparency and engagement with Individual's for those wishing to exercise their rights with regard to personal data and such enquiries are handled effectively
- Regular reviews of processes and systems involving personal data are carried out
- Privacy by design is adopted for all new and changed systems and processes

As part of the ongoing management processes within Scope HR Solutions data protection and the use of personal data is reviewed on an ongoing basis with structured internal audits and reviews quarterly.

Scope HR Solutions Limited are committed to GDPR Compliance.