Data Protection Policy

1. Purpose

The company is required to process relevant personal data regarding the employees, principals, suppliers and customers as part of its operation and shall take all reasonable steps to do so in accordance with this Policy.

2. Main Principles

The company comply with the "Principles relating to processing of personal data" (the Principles) as these are summarized in Article 5 of the GDPR. In accordance with Article 5 the management of personal data is carried out as follows:

a. Lawfulness, fairness, and transparency: personal data are processed lawfully, fairly, and in a transparent manner
b. Limited purpose: personal data are collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes
c. Data minimization: personal data are adequate, relevant, and limited to which it is necessary in relation to the purposes for which they are collected
d. Accuracy: personal data that stored and managed are accurate and, where necessary, kept up to date
e. Storage limitation: personal data are kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.
f. Confidentiality and integrity: personal data are processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures
g. Accountability: Data Protection Officer (DPO) is responsible for demonstrating compliance with the Data Protection principles.

3. Compliance With GDPR

Data Protection Officer (DPO)

The company has appointed the **HR Manager** as the Data Protection Officer (DPO) who will endeavour to ensure that all personal data is processed in compliance with this Policy and the Principles of the Data Protection Act 1998. The Freedom of Information Act 2000 and the Protection of Freedoms Act 2012 are also relevant to parts of this policy.

The company recognizes The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) adopted 27 April 2016, the two-year transition period and the application date of 25 May 2018 and is actively working towards compliance with that directive.

DPO is the sole employee / officer that has access to Company's Employees Data Records (QEFS-04).

Personal Data

Personal data covers both facts and opinions about an individual where that data identifies an individual. For example, it includes information necessary for employment such as the member of staff's name and address and details for payment of salary / contracts, training etc. Personal data may also include sensitive personal data as defined in the Act.

Processing of Personal Data

Consent may be required for the processing of personal data unless processing is necessary for the performance of the contract of employment. Any information which falls under the definition of personal data and is not otherwise exempt, will remain confidential and will only be disclosed to third parties with appropriate consent.

Sensitive Personal Data

The company may, from time to time, be required to process sensitive personal data. Sensitive personal data includes data relating to medical information, gender, religion, nation, trade union membership and criminal records and proceedings.

Transfer of Data

We will not transfer your data to third parties as a matter of course without letting you know in advance or asking for your prior permission. We may only transfer employees' data to third parties without informing you separately beforehand in the following exceptional cases as explained below:

a. If required for investigating the illegal use of UMAR WSR or for legal proceedings, personal data will be transferred to the criminal investigation authorities and, if appropriate, to injured third parties. We will only do this if there are concrete indications of illegal and/or abusive behaviour. We can only transfer on your personal data if this is used to enforce General Terms and Conditions of Business or other agreements. We are also legally obliged to give certain public authorities information. These are criminal investigation authorities, public authorities which prosecute administrative offences entailing fines and the German finance authorities.

b. Occasionally we depend on contractually affiliated external companies and external service providers to supply services such as the supply of advertising measures (only if you have given your explicit prior consent), processing payments (PayPal, credit card etc.), storing your data and customer service. In such cases, information is transferred to these companies or individuals in order to enable them to process this information further. We carefully select these external service providers and review them regularly to ensure that your privacy is preserved. The service providers may only use the data for the purposes stipulated by us. We also contractually require the service providers to treat your data solely in accordance with this Privacy Policy and the GDPR.

c. In order to further develop our business, we may alter the corporate structure of UMAR WSR by changing its legal form. We may also form, sell or buy subsidiaries, divisions or parts of the company. In such transactions, customer information together with the part of the company to be transferred will be passed on. Every time personal data are transferred to third parties to the extent prescribed, company will ensure that this is done in accordance with this Privacy Policy and the GDPR.

Newsletter

UMAR WSR provides a newsletter service free of charge. We use the newsletter to inform you about new products and send you general information about UMAR WSR. We need your email address in order to send you the newsletter. We will store and use your email address solely to send you the newsletter.

Of course, you can unsubscribe the newsletter at any time. Every newsletter contains the information on how you can unsubscribe the newsletter with effect for the future.

Rights of Access to Information

Data subjects have the right of access to information held by the company, subject to the provisions of the Data Protection Act 1998 and the Freedom of Information Act 2000. Any data subject wishing to access their personal data should put their request in writing to the DPO. The company will endeavour to respond to any such written requests as soon as is reasonably practicable and in any event, within 30 days for access to records. The information will be imparted to the data subject as soon as is reasonably possible after it has come to the company's attention and in compliance with the relevant Acts.

Accuracy

The company will endeavour to ensure that all personal data held in relation to all data subjects is accurate. Data subjects must notify the data processor of any changes to information held about them. Data subjects have the right in some circumstances to request that inaccurate information about them is erased. This does not apply in all cases, for example, where records of mistakes or corrections are kept, or records which must be kept in the interests of all parties to which they apply.

Enforcement

If an individual believes that the company has not complied with this Policy or acted otherwise than in accordance with the Data Protection Act, the member of staff should utilize the company grievance procedure (QEF-09 Open Reporting System) and should also notify the DPO.

Data Security

The company has taken appropriate technical and organizational steps to ensure the security of personal data. In case of any undesirable breach the company will make all the necessary arrangements for recurrence informing the Data Protection Authorities (QEP-10, GDPR BREACH RESPONSE)

All staff will be made aware of this policy and their duties.

The company and therefore all employees are required to respect the personal data and privacy of others and must ensure that appropriate protection and security measures are taken against unlawful or unauthorized processing of personal data, and against the accidental loss of, or damage to all personal data.

An appropriate level of data security must be deployed for the type of data and the data processing being performed. In most cases, personal data are stored in the server. Other personal data may be for publication or limited publication within the company, therefore having a lower requirement for data security.

Attention is also drawn to the existence of the Computer Network and Internet Access Policy, which provides more specific information on digital data protection.

External Processors

The company ensures that data processed by external processors, for example, service providers, Cloud services including storage, web sites etc. are compliant with this policy and the relevant legislation.

Secure Destruction

When data held in accordance with this policy is destroyed, it must be destroyed securely in accordance with best practice at the time of destruction.

Retention of Data

The company retain data for differing periods of time for different purposes as required by statute or best practices, individual departments incorporate these retention times into the processes and manuals. Other statutory obligations, legal processes and enquiries may also necessitate the retention of certain data.

The company may store some data such as registers, photographs, exam results, achievements, books and works etc. indefinitely in its archive.

Deleting Your Data

If your data are no longer required for the aforementioned purposes, we will delete them. If data has to be retained for statutory reasons, these will be blocked and will then no longer be available for any further use.

CCTV

The company owns and operates a CCTV network for the purposes of crime prevention and detection and Safeguarding. The CCTV network has been declared to the state local authorities. Where a data subject can be identified, images must be processed as personal data.