DATA PROTECTION POLICY

Markwatch Data  Protection Policy

Data Protection

Data protection is the safeguarding of the privacy rights of individuals in relation to the processing of their personal data. The Data Protection Acts and guidelines issued by the Irish GDPR provide rights to individuals relating to this personal information and impose obligations on organisations who collect and use personal data. Markwatch is preparing to be fully compliant with the GDPR requirements during the year 2018. We collect, use and retain personal data and information (for as long as is necessary for the purpose or purposes for which it was obtained) for a variety of necessary purposes about its staff, Learners and other relevant individuals. Data is collected for the following purposes:

- Organisation and administration of programmes including processing of assessment s/ results
- QQI requirements for certification
- External evaluation activities
- Recruitment and remuneration of staff
- Compliance with legal obligations to regulatory bodies etc.

If the purpose for which the information was obtained has ceased and the personal information (such as PPS numbers) is no longer required, Markwatch discards/ deletes the data in a secure manner.

Markwatch may also provide promotional and marketing materials to individuals who have provided personal information such as email addresses. Individuals may also remove themselves from all mailing lists generated by Markwatch. We are in the process of publishing our data protection guidelines and also to institute a system of obtaining individual consent in all cases.

New GDPR Legislation and Key Changes:

Markwatch is conscious of the new GDPR Legislation becoming effective in Ireland on 25 May 2018. Markwatch is in the process of formulating combined necessary documentation for GDPR to meet the requirements of both the Markwatch Security Training Services and the Markwatch Security Business. The key changes that the new GDPR Legislation imposes are as listed below, are being catered for in the new GDPR policy documentation:

Increased Territorial Scope (extra-territorial applicability)

Arguably the biggest change to the regulatory landscape of data privacy comes with the extended jurisdiction of the GDPR, as it applies to all companies processing the personal data of data subjects residing in the EU, regardless of the company's location.

Penalties

Under GDPR organizations in breach of GDPR can be fined up to 4% of annual global turnover or €20 Million (whichever is greater). There is a tiered approach to fines e.g. a company can be fined 2% for not having their records in order (article 28), not notifying the supervising authority and data subject about a breach or not conducting impact assessment. It is important to note that these rules apply to both controllers and processors -- meaning 'clouds' will not be exempt from GDPR enforcement.

Consent

The conditions for consent have been strengthened, and companies will no longer be able to use long illegible terms and conditions full of legalese, as the request for consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent.

Data Subject Rights

Breach Notification

Under the GDPR, breach notification will become mandatory & must be done within 72 hours of first having become aware of the breach.

Right to Access

Part of the expanded rights of data subjects outlined by the GDPR is the right for data subjects to obtain from the data controller confirmation as to whether or not personal data concerning them is being processed, where and for what purpose. This change is a dramatic shift to data transparency and empowerment of data subjects.

Right to be Forgotten

Also known as Data Erasure, the right to be forgotten entitles the data subject to have the data controller erase his/her personal data.

Data Portability

GDPR introduces data portability - the right for a data subject to receive the personal data concerning them, which they have previously provided in a 'commonly use and machine readable format' and have the right to transmit that data to another controller.

Privacy by Design

Privacy by design as a concept has existed for years now, but it is only just becoming part of a legal requirement with the GDPR. Article 23 calls for controllers to hold and process only the data absolutely necessary for the completion of its duties (data minimisation), as well as limiting the access to personal data to those needing to act out the processing.

Data Protection Officers (DPO)

There will be internal record keeping requirements and DPO appointment will be mandatory only for those controllers and processors whose core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale or of special categories of data or data relating to criminal convictions and offences.

Disclosure to Third Parties

Sensitive information may in some cases be disclosed to third parties such as QQI where it is legally required (for example, when necessary to register Learners and when processing their assessments or certifications). In the case of Learners who have enrolled on programmes through their employers, their data (such as attendance and assessment results) may be shared with the employer.

Data Collection and Management

Personal Data

Personal identifying information on all learners is gathered and maintained for the purpose of providing an individually tailored service to each learners , and for registering learners for certification with accrediting bodies.

This information is collected for each individual learner as part of the application process. All personal learners' information collected through these processes (i.e. name(s), addresses, email, contact telephone numbers, PPSN, gender, nationality, country of birth, occupational status.) is inputted into Markwatch System. All learners will be facilitated to register a change in their personal details at any stage of their studies. To facilitate a name-change, learners are required to submit suitable identification/documentation with the desired name (i.e. birth certificate/marriage certificate). This documentation will be forwarded to the relevant accrediting body and maintained on file by Markwatch.

At the application/registration stage, learners are also informed of Markwatch's obligation to share this information with QQI/Other relevant bodies.

Additional hardcopy documentation gathered in the application process is maintained for the period of registration of the individual learners . This can include:

- Application form

- Photographs

- Copy of ID (drivers license/ passport)

- Copy of visa (International learners)

- English proficiency evidence (International learners)

Tutorial information, which may be required even after learners have graduated, is maintained by Markwatch indefinitely. This information may be relevant to learners who progress to further education or who appeal assessment results to the accrediting bodies, for example. Currently the following records are maintained indefinitely by Markwatch:

- All formal written correspondence between tutors and learners ;

- All original documentation relating to additional supports or assessment accommodations implemented (e.g. for reasons of disability/medical condition/specific learning difficulty);

- Records of assessment appeals and outcomes;

- Records of disciplinary procedures and outcomes (including any plagiarism investigations).

Specific purpose and uses of the learner information by Markwatch

Markwatch prepares a portfolio for each learner, essentially consisting of their registration forms, contact details and their personal IDs. This information is used only for the following purposes:

- To assess their eligibility for the selected programmes

- To share this information with the awarding body (QQI) and the regulating body (PSA) for processing of assessments, certifications and licensing.

- To maintain contact with them and provide them access to the online platforms when required

- To carry out follow-up contact and advice-service after they complete their programmes with Markwatch

- To use it for any other purposes, if agreed with the learner

- To retain it for a maximum of 3 years as currently required by the awarding body (QQI) and the regulating body (PSA).

Consent

Based on the conditions for consent as laid down in the GDPR the request for consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent. In the case of Markwatch, the learner’s consent is obtained on their Registration Forms which also explain the purposes for which that information is used, which include sharing of their data with QQI/PSA/An Garda Siochana etc.

Academic Performance and Achievement

Details of programmes, modules and assessments completed by learners are recorded by Markwatch and maintained indefinitely, to facilitate the certification of learners' work through the accrediting bodies as well as facilitating access, transfer and progression for learners .

All marks/grades achieved by learners in assessments are recorded and maintained in secure environment on Markwatch system and on the QBS, which are updated on completion of each module. Internal result-sheets are produced and these are finalised and signed on conclusion of the Results Approval Panel meeting. Following the meeting the agreed marks are signed off by the Academic Committee on the QQI's QBS for issuing of certificates.

For each module of their studies with Markwatch , each learner's work is securely stored by their Tutor. This includes:

 All work submitted by the learners for assessment;

 Copy of written feedback given to learners on assignments;

 Copies of appropriate documentation regarding assessment supports and/or accommodations implemented;

 Records of assessment appeals and outcomes.

Learners' Feedback

Learners' satisfaction with and feedback on the programmes and services of Markwatch is garnered through a series of module and end of programme feedback sessions. In these feedback sessions, learners are invited to give their feedback on the module and programme content and delivery, the tutorial and other learning supports, and the subsidiary support services offered by Markwatch .

This feedback is treated as confidential and identifying information of respondents is not contained in any published material. However in the case of inappropriate use of the feedback sessions, individual responses may be altered or removed, as deemed appropriate by Markwatch. Inappropriate use of the feedback sessions includes the identification of any staff member or learner/s by using their name in a response, and the use of language that may be considered defamatory, obscene, threatening or offensive. Learners are provided with appropriate usage guidelines before commencing any feedback sessions.

Progression Data

Markwatch administers surveys with graduates at intervals of one, three and five years following their graduation, in accordance with the procedures described previously. The purpose of these surveys is to gather data on graduates academic

and career progression routes and to assess continuing training and education needs of graduates.

Critical Quality Indicators

All of the data gathered by Markwatch provides important information to Markwatch about the success of its endeavours, areas requiring improvement and opportunities for further developments. All data which is considered to be a critical quality indicator is carefully considered by the MD/Academic committee, and forms the basis upon which recommendations are made to amend, develop and improve our programmes. Data, which is considered to be a critical quality indicator, includes:

- Learners' registration numbers
- Withdrawal numbers
- Completion rates
- Assessment results
- Staff and learners' feedback
- Quality assurance recommendations and follow-up

Definitions used in the Data Protection Acts

The following definitions have been adapted from the existing Data Protection Acts:

- *Data* means automated and manual data. Automated data means any information on computer, or information recorded with the intention that it be processed by computer. Manual data means information that is recorded as part of a relevant filing system or with the intention that the data form part of a system.

- *Data Controller* means a body that, either alone or with others, controls the contents and use of personal data.

- *Data Processor* means a person who processes personal data on behalf of a data controller but does not include an employee of a data controller who processes such data in the course of his employment.

- *Data Subject* means an individual who is the subject of personal data.

- *Personal Data* means data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller.

- *Processing* means performing any operation or set of operations on the information or data, whether or not by automatic means, including:

    - o Obtaining, recording or keeping the information, or

    - o Collecting, recording organising, storing, altering or adapting the information or data,

o Retrieving, consulting or using the information or data

o Disclosing the information or data by transmitting, disseminating or otherwise making them available, or

o Aligning, combining, blocking, erasing or destroying the information or data.

 Relevant Filing System means any set of information relating to individuals to the extent that, while not computerised, is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.

 Sensitive Personal Data means personal data which relate to specific categories defined as:

o The racial or ethnic origin, the political opinions or the religious or philosophical beliefs of the data subject

o Trade union membership

o The physical or mental health or sexual life of the data subject

o The commission or alleged commission of any offence by the data subject or

o Any proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.

Data Protection Principles

Eight Data Protection Principles are set out in the Data Protection Acts, which Markwatch recognises and adheres to as good practice principles:

(i) *Obtain and process information fairly*

Markwatch will obtain and process personal data fairly and in accordance with the fulfilment of its functions.

(ii) *Keep data only for one or more specified, explicit and lawful purposes*

Markwatch will keep data for purposes that are specific, lawful and clearly stated and the data will only be processed in a manner compatible with these purposes.

(iii) *Use and disclose data only in ways compatible with these purposes*

Markwatch will only disclose personal data that are necessary for the purpose(s) or compatible with the purpose(s) for which it collects and keeps the data.

(iv) *Keep data safe and secure*

Markwatch will take appropriate security measures against unauthorised access to, or alteration, disclosure, destruction or unlawful processing of the data and against accidental loss or destruction.

(v) *Keep data accurate, complete and, where necessary, up-to-date*

Markwatch will have procedures that are adequate to ensure high levels of data accuracy and will put in place appropriate procedures to keep data up-to-date.

(vi) *Ensure that data are adequate, relevant and not excessive*

Personal data held by Markwatch will be adequate, relevant and not excessive in relation to the purpose(s) for which it is collected and kept.

(vii) *Retain data for no longer than is necessary for the purpose or purposes*

Markwatch will develop a policy on retention periods for personal data of learners .

(viii) *Give a copy of his/her personal data to that individual, on request, and correct the data or, in certain cases as defined in the Data Protection Acts, block or erase the data where that individual so requests*

Markwatch will have procedures in place to ensure that data subjects can exercise their rights under the Data Protection legislation.

Responsibility

All employees of Markwatch who collect and/or control the contents and use of personal data are responsible for compliance with the Data Protection principles. It will be the responsibility of the MD to develop and encourage good information handling practices within Markwatch .

Procedures and Guidelines

This policy supports the provision of a structure to assist in Markwatch 's compliance with the Data Protection principles, including the provision of best practice guidelines and procedures in relation to all aspects of Data Protection. 125 of 131

Status of this Policy

This Policy has been approved by Markwatch Management and applies to all staff and learners of Markwatch . Any breach of the Data Protection principles or this Policy will be taken seriously and may result in disciplinary proceedings.

Any member of staff or learners of Markwatch who considers that the Policy has not been followed in respect of personal data about themselves should raise the matter immediately with their directors/tutors in the first instance.

Review

This Policy will be kept under review in light of new legislative/administrative changes which may be implemented over time by the Data Commissioner in view of the new GDPR indicators.