

Data Protection Policy

Triagon Academy Ltd.

Controller: Triagon Academy Ltd.
Data Protection Officer: AKWISO LTD
Approved by: Senate
Review cycle: Annual

Contents

I.	Foundational Provisions.....	3
§1	Purpose and Scope	3
§2	Legal Framework	3
§3	Controller and Data Protection Officer	3
§4	Definitions	4
II.	Principles of Processing.....	6
§5	Data Protection Principles.....	6
§6	Legal Bases for Processing	6
§7	Consent.....	7
§8	Erasure and Storage Duration	7
III.	Processing of Personal Data at Triagon	8
§9	Categories of Data Subjects and Purposes	8
§10	Online Registration and Study Contract.....	8
§11	Contact Form and E-mail Contact.....	9
§12	Newsletter and Marketing Communications	9
§13	Research Data	10
§14	Staff Data	10
IV.	Website, Cookies and Online Services.....	11
§15	Provision of the Website and Log Files.....	11
§16	Use of Cookies.....	11
§17	Web Analysis (Google Analytics)	12
§18	Embedded Content, Social Media and Advertising Services	12
§19	Customer Relationship Management (HubSpot)	13
§20	Links to External Websites.....	14
V.	Recipients, Transfers and Security	15
§21	Recipients and Processors	15
§22	International Data Transfers	15
§23	Security of Processing	15
§24	Personal Data Breaches	16
VI.	Rights of Data Subjects	17
§25	Overview of Rights.....	17
§26	Right of Access	17
§27	Right to Rectification	18
§28	Right to Restriction of Processing.....	18
§29	Right to Erasure	18
§30	Right to Notification	19
§31	Right to Data Portability	19
§32	Right to Object	20
§33	Right to Withdraw Consent	20
§34	Automated Individual Decision-Making, including Profiling	20
§35	Right to Lodge a Complaint with a Supervisory Authority.....	21
§36	Exercising Rights	21
VII.	Fundamental Regulations	23
§37	Responsibilities and Compliance	23
§38	Review	23

I. Foundational Provisions

§1 Purpose and Scope

- (1) The protection of personal data is important to Triagon. This Policy sets out how Triagon Academy Ltd. (Triagon) processes personal data in accordance with applicable European and national legislation, what data is collected, how it is used and shared, what security measures are taken to protect it, and how data subjects can exercise their rights.
- (2) This Policy applies to all personal data processed by Triagon, including the data of applicants, students, alumni, staff, research participants, partners, and users of Triagon's website and online services. It applies to all staff and to all persons and service providers who process personal data on Triagon's behalf.
- (3) This Policy is to be read in conjunction with the Faculty and Staff Policy (§21 and §25), the Employee Handbook (Section IX), the Information Technology Policy (§4), the Research Ethics Policy and Triagon's records retention schedule. In case of conflict, applicable data protection legislation prevails.

§2 Legal Framework

- (1) Personal data is processed in accordance with:
 - Regulation (EU) 2016/679, the General Data Protection Regulation (GDPR);
 - the Data Protection Act (Cap. 586 of the Laws of Malta) and the regulations made under it;
 - the rules on the confidentiality of electronic communications, cookies and electronic direct marketing applicable in Malta; and
 - any other applicable European and national legislation.

§3 Controller and Data Protection Officer

- (1) The controller within the meaning of the GDPR and other applicable data protection legislation is:

Controller	
Name	Triagon Academy Ltd.
Address	Villa Violette, Triq San Bernard, Marsa MRS 1331, Malta
Telephone	+356 7970 6849
E-mail	glen.farrugia@triagon.mt
Website	www.triagon.mt

(2) The Data Protection Officer appointed by the controller is:

Data Protection Officer	
Name	AKWISO LTD, Data Protection and IT Security
Contact person	Dieter Grohmann
E-mail	info@akwiso.com
Website	www.akwiso.com

(3) Data subjects may contact the controller or the Data Protection Officer at any time, by e-mail or by post, on any matter relating to the processing of their personal data or the exercise of their rights.

§4 Definitions

(1) This Policy uses the terminology of the GDPR. For ease of reading, the most important terms are explained below:

- **Personal data** means any information relating to an identified or identifiable natural person (the data subject). A person is identifiable if he or she can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or one or more factors specific to his or her physical, physiological, genetic, mental, economic, cultural or social identity.
- **Data subject** means any identified or identifiable natural person whose personal data is processed by the controller.
- **Processing** means any operation or set of operations performed on personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation, retrieval, consultation, use, disclosure, alignment or combination, restriction, erasure or destruction.
- **Profiling** means any form of automated processing of personal data used to evaluate personal aspects of a natural person, in particular to analyse or predict aspects concerning that person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
- **Pseudonymisation** means processing personal data in such a way that it can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures.
- **Controller** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

- **Processor** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
- **Recipient** means a natural or legal person, public authority, agency or other body to which personal data is disclosed, whether a third party or not. Public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law are not regarded as recipients.
- **Third party** means a natural or legal person, public authority, agency or body other than the data subject, the controller, the processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.
- **Consent** means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a 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.

II. Principles of Processing

§5 Data Protection Principles

- (1) Triagon processes personal data in accordance with the principles set out in Article 5 GDPR. Personal data shall be:
 - processed lawfully, fairly and in a transparent manner;
 - collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes;
 - adequate, relevant and limited to what is necessary for the purposes of processing;
 - accurate and, where necessary, kept up to date;
 - kept in a form which permits identification of data subjects for no longer than is necessary; and
 - processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.
- (2) Triagon is responsible for, and must be able to demonstrate, compliance with these principles.

§6 Legal Bases for Processing

- (1) Where Triagon obtains the consent of the data subject for the processing of personal data, Art. 6(1)(a) GDPR serves as the legal basis.
- (2) Where the processing of personal data is necessary for the performance of a contract to which the data subject is a party, such as a study contract or an employment contract, Art. 6(1)(b) GDPR serves as the legal basis. This also applies to processing necessary for steps taken prior to entering into a contract.
- (3) Where the processing of personal data is necessary for compliance with a legal obligation to which Triagon is subject, Art. 6(1)(c) GDPR serves as the legal basis.
- (4) Where the processing is necessary for the purposes of the legitimate interests pursued by Triagon or by a third party, and the interests, fundamental rights and freedoms of the data subject do not override those interests, Art. 6(1)(f) GDPR serves as the legal basis.
- (5) Special categories of personal data, such as data concerning health, are processed only where one of the conditions in Art. 9(2) GDPR applies, for example where the data subject has given explicit consent or the processing is necessary for obligations in the field of employment law.

§7 Consent

- (1) Where processing is based on consent, the data subject may withdraw consent at any time with effect for the future. Withdrawal does not affect the lawfulness of processing carried out on the basis of consent before its withdrawal.
- (2) To withdraw consent, the data subject may contact the controller or the Data Protection Officer (§3).

§8 Erasure and Storage Duration

- (1) The personal data of the data subject is erased or blocked as soon as the purpose of storage ceases to apply. Personal data may be stored for longer where this is provided for by European or national legislation to which Triagon is subject.
- (2) Personal data is also blocked or erased when a storage period prescribed by such legislation expires, unless further storage is necessary for the conclusion or performance of a contract.
- (3) Specific storage periods are set out in the relevant provisions of this Policy and in Triagon's records retention schedule. They include the following:

Category of data	Storage period
Website log files (§15)	Up to seven days; any longer storage only with IP addresses erased or anonymised
Technical data collected when sending a contact form (§11)	Up to seven days
Contact enquiries (§11)	Until the enquiry has been conclusively resolved
Address, payment and contract data (§10)	Ten years after performance of the contract, as required by commercial and tax regulations; processing restricted after two years
Voluntarily provided registration data (§10)	Two years after performance of the last contract
Customer relationship management data (§19)	Twelve months, unless a longer period is required by law
Student academic records and staff records	As set out in Triagon's records retention schedule

III. Processing of Personal Data at Triagon

§9 Categories of Data Subjects and Purposes

- (1) Triagon processes personal data in particular for the following purposes:
- **Applicants and students:** admission, enrolment and the study contract; teaching, supervision and assessment through the virtual learning environment; examinations and the award of qualifications; student support; and quality assurance, including student feedback and alumni tracer studies.
 - **Staff:** recruitment, employment, payroll, performance and professional development, in accordance with the Faculty and Staff Policy. Employee data is managed in the HR platform Personio.
 - **Research participants:** research conducted by staff and students, subject to prior ethics clearance under the Research Ethics Policy (§13).
 - **Prospective students, website users and other contacts:** providing the website and online services, answering enquiries and, with consent, marketing communications.

§10 Online Registration and Study Contract

- (1) Users may register on Triagon's website by providing personal data. The data is entered into an input mask, transmitted to Triagon and stored. During registration the e-mail address, IP address and the date and time of registration are collected. Registration uses a double opt-in procedure: after registration, an e-mail is sent asking the user to confirm the registration. If the registration is not confirmed within 48 hours, the data is blocked and automatically deleted after one month. The IP address and the times of registration and confirmation are stored in order to prove the registration and, where necessary, to clarify any misuse of personal data.
- (2) Where a user registers for a study programme or other service, the personal data required to process the registration and perform the contract is collected. Mandatory information is marked; further information is voluntary. The data collected includes surname, address (and any differing billing address), e-mail address, telephone number, bank details, IP address, and the date and time of data entry.
- (3) Personal data is disclosed to third parties only where this is necessary for the performance of the contract, for billing or for the collection of fees, or where the data subject has expressly consented. Only the data required in each case is disclosed. Recipients may include:
- collection companies, where a payment has to be recovered (name, address and contract details);
 - the bank processing the payment, where payment is made by direct debit; and
 - accounting services.

- (4) The legal basis for processing mandatory data is Art. 6(1)(b) GDPR; for voluntary data it is Art. 6(1)(a) GDPR.
- (5) Due to commercial and tax regulations, address, payment and contract data is stored for ten years after performance of the contract; after two years, processing is restricted to compliance with legal obligations. Where there is a continuing contractual relationship, the data is stored for the entire contract period and for ten years thereafter. Voluntarily provided data is deleted two years after performance of the last contract. Statutory retention periods take precedence.
- (6) Where data is required for the performance of a contract, early deletion is possible only insofar as contractual or legal obligations do not preclude it. Otherwise, the data subject may request the deletion or correction of the data at any time by contacting the controller or the Data Protection Officer (§3).

§11 Contact Form and E-mail Contact

- (1) A contact form is available on the website. Where it is used, the data entered (first name, last name, telephone number, e-mail address, country and the request) is transmitted to Triagon and stored. At the time the message is sent, the user's IP address and the date and time are also stored. Consent to this processing is obtained during the sending process, with reference to this Policy.
- (2) Alternatively, Triagon may be contacted by e-mail, in which case the personal data transmitted with the e-mail is stored. Where contact details are provided, Triagon may use the same channel to respond to the enquiry. The data is used exclusively for handling the enquiry and is not disclosed to third parties.
- (3) The legal basis for processing data entered in the contact form is Art. 6(1)(a) GDPR. The legal basis for processing data transmitted by e-mail is Art. 6(1)(f) GDPR. Where the contact aims at the conclusion of a contract, Art. 6(1)(b) GDPR is an additional legal basis.
- (4) The data is deleted when the enquiry has been conclusively resolved. The additional data collected during the sending process is deleted after seven days at the latest.
- (5) The data subject may withdraw consent or object to the storage of the data at any time by contacting the controller or the Data Protection Officer (§3). In that case, the enquiry cannot be continued and all personal data stored in connection with it is deleted.

§12 Newsletter and Marketing Communications

- (1) With consent, users may subscribe to Triagon's free newsletter, which provides information about current offers. Subscription uses a double opt-in procedure: after subscribing, the user receives an e-mail asking for confirmation. If the subscription is not confirmed, the data is blocked and automatically deleted after

one month. The IP address and the times of subscription and confirmation are stored in order to prove the subscription and to clarify any misuse.

- (2) The only mandatory information is the e-mail address. Any further information is voluntary and is used to address the subscriber personally. The data is used exclusively for sending the newsletter.
- (3) The legal basis for processing is Art. 6(1)(a) GDPR, together with the rules on electronic direct marketing applicable in Malta.
- (4) The e-mail address is stored for as long as the subscription is active. Subscribers may unsubscribe and withdraw consent at any time using the unsubscribe link in each newsletter or by contacting the controller (§3).

§13 Research Data

- (1) Personal data collected in research by staff, doctoral candidates and students is processed only after ethics clearance has been granted in accordance with the Research Ethics Policy, and only for the purposes approved.
- (2) Research data is stored in approved institutional systems, pseudonymised or anonymised wherever possible, and processed in accordance with the Research Strategy (Section 8.3). The exceptions for scientific research in Art. 89 GDPR apply only subject to appropriate safeguards.

§14 Staff Data

- (1) Personal data of applicants for employment and of staff is processed for recruitment, the performance of the employment contract, compliance with legal obligations and the administration of professional development, in accordance with the Faculty and Staff Policy (§25).
- (2) All staff must handle personal data in accordance with this Policy and the practical rules set out in the Employee Handbook (Section IX).

IV. Website, Cookies and Online Services

§15 Provision of the Website and Log Files

- (1) When the website is used for information purposes only, the following data is automatically collected from the accessing device each time the website is accessed:
 - the IP address of the user;
 - the browser type and version, and the language and version of the browser software;
 - the operating system of the user;
 - the internet service provider of the user;
 - the date and time of access;
 - the websites from which the user's system accesses the website, and the websites accessed via the website;
 - the content accessed (specific pages) and the amount of data transferred.
- (2) This data is stored in the log files of Triagon's systems. It is not stored together with other personal data of the user.
- (3) The temporary storage of the IP address is necessary to deliver the website to the user's device for the duration of the session. Storage in log files ensures the functionality and security of the website and of Triagon's information technology systems and, in the event of a cyber-attack, allows information to be provided to law enforcement authorities. The data is not evaluated for marketing purposes in this context.
- (4) The legal basis is Art. 6(1)(f) GDPR, based on Triagon's legitimate interest in the purposes described in paragraph (3).
- (5) The data is deleted as soon as it is no longer required, and log file data after seven days at the latest. Any longer storage takes place only with IP addresses deleted or anonymised so that the accessing client can no longer be identified.
- (6) The collection of data for the provision of the website and its storage in log files is essential for the operation of the website; there is therefore no possibility to object.

§16 Use of Cookies

- (1) The website uses cookies. Cookies are small text files that are stored on the user's device (computer, tablet, smartphone or similar) when a website is visited. Some cookies contain a characteristic string (cookie ID) that enables the browser to be recognised when the website is visited again.

- (2) Technically necessary cookies make the website usable and enable certain functions, such as language settings, log-in information, the online study contract and remembering search terms. The user data collected through these cookies is not used to create user profiles. The legal basis is Art. 6(1)(f) GDPR, and the storage of such cookies is permitted as strictly necessary for the service requested by the user.
- (3) Analysis and marketing cookies are used to understand how the website is used and to improve its quality and content. They may process data such as search terms entered, the frequency of page views and the use of website functions. Where possible, such data is pseudonymised. These cookies are used only with the user's consent, obtained through the cookie settings displayed when the website is first visited. The legal basis is Art. 6(1)(a) GDPR. Consent may be withdrawn at any time through the cookie settings.
- (4) Users have full control over the use of cookies and can configure their browser to be notified when cookies are set, to refuse cookies in general, or to delete cookies individually. Disabling cookies may limit the functionality of the website. Session cookies are deleted automatically when the browser is closed.

§17 Web Analysis (Google Analytics)

- (1) With the user's consent, the website uses Google Analytics, a web analysis service provided by Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland, to analyse how users use the website. Google Analytics uses cookies to collect information such as the pages visited, entry and exit pages, the length of visit, the frequency of visits, the approximate region of origin, language, browser, operating system and screen resolution, and the search terms and search engines used.
- (2) Google Analytics is configured so that IP addresses are not stored in full. Information may be transferred to servers of Google LLC in the United States; such transfers take place on the basis of the EU-US Data Privacy Framework or other safeguards under Art. 44 et seq. GDPR (§22).
- (3) On Triagon's behalf, Google uses this information to evaluate the use of the website and to compile reports on website activity, which help Triagon improve the website and its user-friendliness.
- (4) The legal basis is Art. 6(1)(a) GDPR. Users may withdraw their consent at any time through the cookie settings, delete cookies already stored, or install the browser add-on for deactivating Google Analytics provided by Google. The data is deleted as soon as it is no longer required for the purposes of analysis.

§18 Embedded Content, Social Media and Advertising Services

- (1) **YouTube.** The website embeds videos from YouTube, a service of Google Ireland Limited, in extended privacy mode. Data about the user is transmitted to YouTube only when a video is played. YouTube may then receive device-specific information, log data (including the IP address, browser type and language, and the date and time of the request) and location-related information, and may link this data to a logged-in Google account.

- (2) **Social media plugins.** The website contains plugins or links to social networks, including Facebook and Instagram (Meta Platforms Ireland Limited), X (formerly Twitter), LinkedIn (LinkedIn Ireland Unlimited Company) and XING (New Work SE). A two-click solution is used wherever possible: no personal data is transmitted to the social network until the user activates the relevant button. Once activated, the network receives information that the user has accessed the page, together with browser-related data such as the IP address, browser type, operating system and time of access, and may link this information to the user's account if the user is logged in. Users who do not wish this should log out of their social network account before activating a plugin.
- (3) **Google Maps and Google Web Fonts.** The website uses Google Maps to display locations and Google Web Fonts for the uniform presentation of fonts. To use these services, the user's IP address is transmitted to Google. The legal basis is Triagon's legitimate interest in an attractive and consistent presentation of its online services (Art. 6(1)(f) GDPR). If the browser does not support web fonts, a standard font is used.
- (4) **Advertising and remarketing.** Where the website uses Google advertising services such as Google AdSense or Google Ads remarketing, these services use cookies and similar technologies, such as counting pixels, to display interest-based advertising and to recognise users who have previously visited the website. These services are used only with the user's consent. Users may also manage interest-based advertising in their Google advertising settings.
- (5) Triagon has no influence on the data collected by the providers referred to in this section, on the purposes and duration of processing, or on the deletion of such data. The providers may store the data as usage profiles and use it for advertising, market research and the design of their services, including for users who are not logged in, and may process it in the United States. Users have the right to object to the creation of such user profiles and must contact the respective provider to exercise it. Further information is available in the providers' own privacy policies.
- (6) Except where stated otherwise in paragraph (3), the legal basis for the use of the services in this section is the user's consent under Art. 6(1)(a) GDPR, which may be withdrawn at any time through the cookie settings.

§19 Customer Relationship Management (HubSpot)

- (1) Triagon uses HubSpot, an integrated software solution for customer relationship management and online marketing. The processor is HubSpot Ireland Limited (HubSpot European Headquarters), Ground Floor, Two Dockland Central, Guild Street, Dublin 1, Ireland. Its data protection officer can be contacted at privacy@hubspot.com.
- (2) HubSpot is used to manage contacts and communication with prospective students and other contacts across several channels (telephone, e-mail, SMS and WhatsApp), with content relating to study

programmes, admissions and Triagon's institutional profile, and through calls, events and newsletters. HubSpot uses web beacons and stores cookies on the user's device.

- (3) The data processed includes the truncated IP address, geographical location, browser type, duration of the visit and pages visited. Processing takes place in the European Union. Only in exceptional cases is the full IP address transferred to a HubSpot server in the United States and truncated there. Transfers are based on the European Commission's adequacy decision for the EU-US Data Privacy Framework (Art. 45 GDPR) and on Standard Contractual Clauses (Art. 46 GDPR).
- (4) The processing is based on Art. 6(1)(a) GDPR, where consent is requested for marketing or tracking measures; on Art. 6(1)(b) GDPR, for example in the case of contact enquiries; and on Art. 6(1)(f) GDPR, based on Triagon's legitimate interest in efficient contact management, communication and the analysis and optimisation of its services. Cookies that are not strictly necessary are used only with consent, which can be withdrawn at any time through the cookie settings.
- (5) Triagon has concluded a data processing agreement with HubSpot in accordance with Art. 28 GDPR. HubSpot processes personal data exclusively on Triagon's instructions.
- (6) Personal data is stored for as long as necessary for the stated purposes and deleted after twelve months, unless consent is withdrawn earlier or statutory retention obligations require longer storage. Further information is available in HubSpot's privacy policy.

§20 Links to External Websites

- (1) The website contains links to external websites. Triagon is responsible only for its own content and has no influence on the content of external websites. When a user follows a link to an external website, the privacy policy of that website applies.
- (2) Users who become aware of unlawful activities or content on a linked website are asked to inform Triagon, which will review the content and act accordingly.

V. Recipients, Transfers and Security

§21 Recipients and Processors

- (1) Personal data is disclosed to recipients only where there is a legal basis for doing so, where this is necessary for the purposes described in this Policy, or where the data subject has consented.
- (2) Triagon uses service providers that process personal data on its behalf, including ISARtec as central IT service provider (Information Technology Policy, §1), the HR platform Personio (§9) and HubSpot (§19). Processors are selected carefully, bound by data processing agreements in accordance with Art. 28 GDPR, and may process personal data only on Triagon's documented instructions.

§22 International Data Transfers

- (1) Personal data is transferred to countries outside the European Economic Area only where the conditions of Art. 44 to 49 GDPR are met, in particular where the European Commission has adopted an adequacy decision, including the EU-US Data Privacy Framework for certified organisations, or where appropriate safeguards such as Standard Contractual Clauses are in place.
- (2) Data subjects may request information about the safeguards applied to such transfers by contacting the controller (§3).

§23 Security of Processing

- (1) Triagon and its processors apply appropriate technical and organisational measures in accordance with Art. 32 GDPR to protect personal data against unauthorised access, loss, misuse, alteration and destruction. Operational IT security is managed within the framework of the security arrangements of Triagon's IT service provider, which is certified to ISO 27001 (Information Technology Policy, §4).
- (2) The website uses SSL/TLS encryption to protect the transmission of confidential content, such as enquiries sent to Triagon. An encrypted connection can be recognised by the prefix "https://" in the browser's address bar and the lock symbol. When encryption is active, data transmitted to Triagon cannot be read by third parties.
- (3) Backups of institutional data are transferred in encrypted form to geo-redundant storage. Access to personal data is restricted to authorised persons who need it for their tasks, and staff receive training in data protection and information security.

§24 Personal Data Breaches

- (1) Any actual or suspected personal data breach must be reported immediately, and in any event within 24 hours, to the Data Protection Officer through the channels set out in the Employee Handbook (Section 9.2).
- (2) Where a breach is likely to result in a risk to the rights and freedoms of natural persons, Triagon notifies the Information and Data Protection Commissioner without undue delay and, where feasible, within 72 hours of becoming aware of it (Art. 33 GDPR). Where the breach is likely to result in a high risk, the data subjects concerned are also informed without undue delay (Art. 34 GDPR).
- (3) All personal data breaches are documented, including their effects and the remedial action taken.

VI. Rights of Data Subjects

§25 Overview of Rights

(1) Where personal data is processed, the data subject has the following rights vis-à-vis the controller:

- the right of access (§26);
- the right to rectification (§27);
- the right to restriction of processing (§28);
- the right to erasure (§29);
- the right to notification (§30);
- the right to data portability (§31);
- the right to object (§32);
- the right to withdraw consent (§33);
- the right not to be subject to automated individual decision-making (§34); and
- the right to lodge a complaint with a supervisory authority (§35).

§26 Right of Access

(1) The data subject may request confirmation from the controller as to whether personal data concerning him or her is being processed. Where this is the case, the data subject may request access, free of charge, to the personal data and to the following information:

- the purposes of the processing;
- the categories of personal data concerned;
- the recipients or categories of recipients to whom the personal data has been or will be disclosed;
- the envisaged period for which the personal data will be stored or, if this is not possible, the criteria used to determine that period;
- the existence of the right to request rectification or erasure, restriction of processing, or to object to such processing;
- the right to lodge a complaint with a supervisory authority;
- where the personal data is not collected from the data subject, any available information as to its source; and
- the existence of automated decision-making, including profiling, referred to in Art. 22(1) and (4) GDPR and, at least in those cases, meaningful information about the logic involved and the significance and envisaged consequences of such processing.

- (2) The data subject has the right to be informed whether personal data is transferred to a third country or to an international organisation and, in that case, of the appropriate safeguards pursuant to Art. 46 GDPR.

§27 Right to Rectification

- (1) The data subject has the right to obtain without undue delay the rectification of inaccurate personal data and the completion of incomplete personal data concerning him or her.

§28 Right to Restriction of Processing

- (1) The data subject may request the restriction of processing of personal data concerning him or her where:
- the accuracy of the personal data is contested, for a period enabling the controller to verify its accuracy;
 - the processing is unlawful and the data subject opposes erasure and requests restriction instead;
 - the controller no longer needs the personal data for the purposes of processing, but the data subject requires it for the establishment, exercise or defence of legal claims; or
 - the data subject has objected to processing pursuant to Art. 21(1) GDPR, pending verification of whether the legitimate grounds of the controller override those of the data subject.
- (2) Where processing has been restricted, such personal data may, with the exception of storage, only be processed with the data subject's consent, for the establishment, exercise or defence of legal claims, for the protection of the rights of another natural or legal person, or for reasons of important public interest of the Union or of a Member State.
- (3) A data subject who has obtained restriction of processing is informed by the controller before the restriction is lifted.

§29 Right to Erasure

- (1) The data subject may require the controller to erase personal data concerning him or her without undue delay where one of the following grounds applies:
- the personal data is no longer necessary for the purposes for which it was collected or otherwise processed;
 - the data subject withdraws consent on which the processing is based according to Art. 6(1)(a) or Art. 9(2)(a) GDPR, and there is no other legal ground for the processing;
 - the data subject objects to the processing pursuant to Art. 21(1) GDPR and there are no overriding legitimate grounds for the processing, or the data subject objects pursuant to Art. 21(2) GDPR;
 - the personal data has been unlawfully processed;

- the personal data must be erased for compliance with a legal obligation under Union or Member State law to which the controller is subject; or
 - the personal data has been collected in relation to the offer of information society services referred to in Art. 8(1) GDPR.
- (2) Where the controller has made the personal data public and is obliged to erase it, the controller, taking account of available technology and the cost of implementation, takes reasonable steps to inform other controllers processing the data that the data subject has requested the erasure of any links to, or copies or replications of, that personal data.
- (3) The right to erasure does not apply to the extent that processing is necessary:
- for exercising the right of freedom of expression and information;
 - for compliance with a legal obligation under Union or Member State law to which the controller is subject, or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
 - for reasons of public interest in the area of public health in accordance with Art. 9(2)(h) and (i) and Art. 9(3) GDPR;
 - for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Art. 89(1) GDPR, insofar as erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
 - for the establishment, exercise or defence of legal claims.

§30 Right to Notification

- (1) Where the data subject has exercised the right to rectification, erasure or restriction of processing, the controller communicates the rectification, erasure or restriction to each recipient to whom the personal data has been disclosed, unless this proves impossible or involves disproportionate effort. The data subject has the right to be informed about those recipients.

§31 Right to Data Portability

- (1) The data subject has the right to receive the personal data concerning him or her, which he or she has provided to the controller, in a structured, commonly used and machine-readable format, and to transmit that data to another controller without hindrance, where:
- the processing is based on consent pursuant to Art. 6(1)(a) or Art. 9(2)(a) GDPR, or on a contract pursuant to Art. 6(1)(b) GDPR; and
 - the processing is carried out by automated means.

- (2) In exercising this right, the data subject has the right to have the personal data transmitted directly from one controller to another, where technically feasible. The rights and freedoms of others must not be adversely affected.
- (3) The right to data portability does not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

§32 Right to Object

- (1) The data subject has the right to object at any time, on grounds relating to his or her particular situation, to the processing of personal data concerning him or her which is based on Art. 6(1)(e) or (f) GDPR, including profiling based on those provisions.
- (2) The controller then no longer processes the personal data unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject, or the processing is for the establishment, exercise or defence of legal claims.
- (3) Where personal data is processed for direct marketing purposes, the data subject has the right to object at any time to such processing, including profiling to the extent that it is related to direct marketing. Following an objection, the personal data is no longer processed for these purposes.
- (4) In the context of the use of information society services, the data subject may exercise the right to object by automated means using technical specifications.

§33 Right to Withdraw Consent

- (1) The data subject has the right to withdraw consent to the processing of personal data at any time. The withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal (§7).

§34 Automated Individual Decision-Making, including Profiling

- (1) The data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. This does not apply if the decision:
 - is necessary for entering into, or the performance of, a contract between the data subject and the controller;
 - is authorised by Union or Member State law to which the controller is subject and which lays down suitable measures to safeguard the data subject's rights, freedoms and legitimate interests; or
 - is based on the data subject's explicit consent.

- (2) Such decisions shall not be based on special categories of personal data referred to in Art. 9(1) GDPR, unless Art. 9(2)(a) or (g) GDPR applies and suitable measures to safeguard the rights, freedoms and legitimate interests of the data subject are in place.
- (3) In the cases referred to in the first and third items of paragraph (1), the controller implements suitable measures to safeguard the data subject's rights, freedoms and legitimate interests, including at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

§35 Right to Lodge a Complaint with a Supervisory Authority

- (1) Without prejudice to any other administrative or judicial remedy, the data subject has the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement, if he or she considers that the processing of personal data relating to him or her infringes the GDPR.
- (2) The supervisory authority in Malta is:

Supervisory authority	
Name	Information and Data Protection Commissioner (IDPC)
Address	Floor 2, Airways House, High Street, Sliema SLM 1549, Malta
Telephone	+356 2328 7100
E-mail	idpc.info@gov.mt
Website	www.idpc.org.mt

- (3) The supervisory authority with which the complaint has been lodged informs the complainant of the progress and outcome of the complaint, including the possibility of a judicial remedy pursuant to Art. 78 GDPR.

§36 Exercising Rights

- (1) Data subjects may exercise their rights at any time by contacting the controller or the Data Protection Officer (§3) by e-mail or by post.
- (2) Triagon responds to requests without undue delay and in any event within one month of receipt. This period may be extended by a further two months where necessary, taking into account the complexity and number of requests, in which case the data subject is informed of the extension and the reasons for it within one month (Art. 12(3) GDPR).

- (3) Information and actions are provided free of charge. Where Triagon has reasonable doubts about the identity of the person making a request, it may request additional information necessary to confirm that person's identity.

VII. Fundamental Regulations

§37 Responsibilities and Compliance

- (1) All staff and all persons processing personal data on behalf of Triagon are required to comply with this Policy.
- (2) Non-compliance may result in disciplinary action in accordance with the Faculty and Staff Policy (§24).
- (3) The Data Protection Officer advises Triagon on its data protection obligations, monitors compliance with this Policy and applicable legislation, and acts as the contact point for data subjects and the supervisory authority.

§38 Review

- (1) This Policy is reviewed annually and whenever material changes occur in applicable legislation, in Triagon's processing activities, or in the services and technologies it uses. Changes to this Policy require the approval of the Senate.
- (2) The current version of this Policy is published on Triagon's website.

Prof. Dr. Dr. Christian Werner

President, TRIAGON