DATA PROTECTION POLICY

Examiz Ltd
71 Baggot Street Lower, D02 P593
Dublin, Ireland
Company No. 674918

Table of contents

I. EXAMIZ LTD.

Examiz Ltd. is a private analytics company located in Dublin, Ireland. It was incorporated in 2020 as a Private Company Limited by Shares. *Examiz Ltd.*, offers diagnostics, applicant tracking and analytics, as well as job-portal services to support recruitments and talent development. Therefore, Examiz sees a need to establish a process to adequately collect and process the respective personal data of applicants and other users.

Thus, *Examiz Ltd.* started to incorporate information-processing technologies using both hardware and software to efficiently store, retrieve, and share user-related information. The implemented services facilitate the use of databases to process large amounts of information, improve personality analytics, and use algorithms that are able to detect specific behaviour patterns.

The following is a description of the procedure included in the package:

Employers and recruiters can define a job-specific profile of personality traits, skills, and personal competencies they find beneficial for a certain job or team. Nominated references provide peer-feedback through an online survey. Once the response data are collected, the data go through the processing platform of *Examiz Ltd*. The platform tries to establish patterns based on the collected data. The establishment of patterns helps the customers to make informed hiring and talent development decisions based on the organisation's needs and improve the performance of staff members and teams.

II. GDPR Principles & Implementation

A. GDPR PRINCIPLES

The adoption of the General Data Protection Regulation (GDPR) by the European Parliament and the EU Council in 2016, means that *Examiz Ltd.* has to design and constantly review a GDPR compliant way the personal data of EU citizens are handled.

The GDPR defines the personal data that require special methods to safeguard it. Its aim is to respect the fundamental rights and protect the personal information of the data subjects.

Chapter 2 of the GDPR lays down in particular the principles and lawfulness of a processing of personal data (Art. 5 and 6 GDPR). According to this, personal data must, for example, only be processed in a lawful and comprehensible manner. There must be a legal basis for the processing of personal data, for example the consent of the data subject or a legal obligation. The data controller must demonstrate compliance with the data protection principles and is therefore accountable.

As a processor, we have created internal processes and structures with the aim of establishing a data protection/information security management system that we continuously develop and thus achieve a continuous improvement in the protection of personal data at Examiz. To this end, as a first step we have set up a data protection and information security team with staff from the technical and legal areas. The team takes care of the definition, implementation and testing of appropriate concepts and processes around data protection and information security management. In addition, we have laid down the goals and principles of internal data protection in a central guideline, which serves to make the importance of the topic clear to all our employees (guideline available on request).

Examiz Ltd. planned and initiated the implementation of the GDPR in of 2020. The first step was to choose a methodical framework to manage the GDPR implementation and to conduct a gap analysis in order to select the most suitable approach to GDPR compliance for the organization. The analysis helped them determine the current situation of the technical and operational measures already in place and assess whether those controls can help the organization achieve the desired results and assess the need for improvement.

Article 37 of the GDPR may require the designation of a data protection officer for organizations whose core activities were on a large scale of special categories of data. However, the gap analysis indicated that at the moment only an extremely limited number personal data is collected and therefore *Examiz Ltd.* does not have to appoint a Datta Protection Office. However, data protection compliance will be the organization's responsibility and with growing service scope and customer base, *Examiz Ltd.* will review or revise this assessment.

Furthermore, *Examiz Ltd.* makes a clear definition of all personal data processing activities by listing the information systems used to process personal data. *Examiz Ltd.* continues the GDPR implementation by

establishing a data protection policy, an incident management process, and a personal data breach response plan.

Examiz Ltd. does not have to have a data protection impact assessment (DPIA) because it does not process a considerable amount of personal data that affects and presents potential risks to a large number of data subjects. However, the steps of the DPIA methodology were followed and actions have been identified to minimize the risk effects regarding personal data processing activities. The actions include the application of technical security measures to a specific data set using encryption and pseudonymization methods.

Examiz Ltd. conducts training and awareness sessions regarding the importance of complying with the GDPR to all *Examiz Ltd.* employees and paid special attention to employees directly involved in data processing activities.

Examiz Ltd. also conducts internal audit regarding the processing of personal data. During the internal audit, *Examiz Ltd.'* compliance is evaluated regarding data subject rights, data protection obligations, the lawful retention of personal data, the implementation of the data protection policy, and the lawful and proper obtainment and processing of personal data.

The internal audits help *Examiz Ltd.* ensure that most of its practices comply with the data protection procedures and processes.

B. GDPR IMPLEMENTATION

a. Transparency & Information (Art. 12, 13, 14 GDPR)

In the context of the new GDPR, we have worked out a privacy policy for our services together with our data protection officer. This allows every user to see which data is processed by us under our own responsibility, which third-party providers are used to provide the services, what we need this data for and what rights users have. Important: Your company's HR data managed in Examiz will only be processed by the subcontractors mentioned in the order processing agreement. The third-party providers mentioned in the privacy policy will not have access to this data.

The privacy policy as well as the imprint of Examiz is directly accessible within the services for every user via the menu bar on the left side and is available in English.

In order to ensure that you fulfil your duty to inform applicants when using the Examiz Recruiting functions, we offer the option of linking your own data protection declaration on your careers page. We will be happy to send you a corresponding template.

For EU citizens: We process all personal date in the EU and do not send personal data outside the European Economic Area. Our servers including backups are located in the EU, currently in Amsterdam, The Netherlands.

b. Right of access of the data subject (Art. 15 GDPR)

Examiz supports you as a company in safeguarding the right to information vis-à-vis your employees and our customers. Users can directly access their own digital personnel file at any time via their own user account and understand which personal data is processed in Examiz.

c. Right of rectification (Art. 16 GDPR)

Employees can request the immediate correction of incorrect personal data at any time. By configuring user roles, Examiz provides you with a comprehensive authorisation concept that allows you to individually define which data your employees are allowed to view or edit.

Via suggestion and editing rights, users can manage selected personnel data themselves and correct them if necessary. Otherwise, it is the responsibility of the respective account administrator to comply with the request for correction.

d. Right to erasure (Art. 17 GDPR)

As soon as the purpose of the data processing becomes obsolete, applicant and employee data must be deleted immediately, taking into account any statutory retention obligations. This is the case, for example, when the employment relationship of an employee who has been assigned a user role in Examiz ends (see also Art. 18 of the GDPR). In this case Examiz allows for a complete deletion of all personal data including all documents managed in Examiz. In the user overview, this process can be carried out for several employees at the same time.

Examiz supports the complete deletion of applicant data. To do this, activate the automatic deletion of applicant data in the recruiting settings. This will irretrievably remove all personal data of cancelled or rejected applicants from Examiz Services after the defined period. Regardless of this, Examiz automatically deletes this data after 18 months at the latest after the application start date. We therefore recommend exporting analysis results and reports from Examiz and including them in the respective personnel file. Anonymised metadata of applicants without personal reference will still be retained for your reporting.

In the event of termination of the business relationship with Examiz, persons authorised to give instructions within your organisation may request the surrender of all data in a machine-readable format. 30 days after termination of the business relationship, your organisation's Examiz account and all related data will be automatically and irretrievably deleted.

e. Right to restriction of processing (Art. 18 GDPR)

According to Art. 18 of the GDPR, in the event of inaccurate data, your employees can ask for the data to be restricted to ensure that it is not inadvertently reused or altered for unwanted purposes.

f. Right to erasure (Art. 17 GDPR)

As soon as the purpose of the data processing becomes obsolete, applicant and employee data must be deleted immediately, taking into account any statutory retention obligations. This is the case, for example, when the employment relationship of an employee who has been assigned a user role in Examiz ends (see also Art. 18 of the GDPR). In this case Examiz allows for a complete deletion of all personal data including all documents managed in Examiz. In the user overview, this process can be carried out for several employees at the same time.

Examiz supports the complete deletion of applicant data. To do this, activate the automatic deletion of applicant data in the recruiting settings. This will irretrievably remove all personal data of cancelled or rejected applicants from Examiz Services after the defined period. Regardless of this, Examiz automatically deletes this data after 18 months at the latest after the application start date. We therefore recommend exporting analysis results and reports from Examiz and including them in the respective personnel file. Anonymised metadata of applicants without personal reference will still be retained for your reporting.

In the event of termination of the business relationship with Examiz, persons authorised to give instructions within your organisation may request the surrender of all data in a machine-readable format. 30 days after termination of the business relationship, your organisation's Examiz account and all related data will be automatically and irretrievably deleted.

g. Right to restriction of processing (Art. 18 GDPR)

According to Art. 18 of the GDPR, in the event of inaccurate data, your employees can ask for the data to be restricted to ensure that it is not inadvertently reused or altered for unwanted purposes.

h. Right to data portability (Art. 20 GDPR)

EU citizens have the right to request all personal data concerning themselves in a structured, commonly used and machine-readable format. Due to Examiz's *MyTalent* self-service approach, applicants can access their own digital file and download documents at any time.

i. Automated individual decision-making, including profiling (Art. 22 GDPR)

EU citizens have the right to be protected protect against carrying out solely automated decision-making that has legal or similarly significant effects on them.

Examiz *does not use* profiling and automated decision-making. Our evaluation and assessment solutions only support decision makers as detailed in our Terms & Conditions. We explicitly forbit the use of our technology for such purposes.

j. Directory of processing activities (Art. 30 GDPR)

According to Art. 30 GDPR, your company as a "controller" must keep a register of all processing activities for which it is responsible. This requirement applies in principle to all companies with more than 250 employees. For companies with less than 250 employees, they only apply to those processing

operations that pose a risk to the rights and freedoms of data subjects or are not only occasional. This is usually the case for all HR and recruiting processes, and therefore also for the use of Examiz Services. For this reason, we have compiled the essential processing activities within the Examiz software in our Data Protection Policy.

k. Security of processing (Art. 32 GDPR)

According to Art. 32 of the GDPR, you as the controller and we as the processor must implement appropriate technical and organisational measures (TOM) for the processing of personal data, which take into account the state of the art, the implementation costs and the risk to the rights and freedoms of data subjects, while ensuring an adequate level of protection. In this context, we have revised our data protection and information security concept and derived additional technical and organisational measures that ensure the confidentiality, integrity, availability and resilience of the systems and services. In future, our new TOM will be directly accessible via the services. The TOM were developed together with our data protection officer and reviewed by him. You can find the audit result on our data protection website.

Migration of the infrastructure to DigitalOcean: In order to guarantee all requirements regarding data protection and IT security and at the same time ensure maximum availability and stability of our software, we will use DigitalOcean for the provision of our IT infrastructure and hosting services in the future.

Encryption of customer data: To ensure that neither DigitalOcean nor any other third parties gain access to customer data, all customer data is stored exclusively in encrypted form. DigitalOcean cannot decrypt or view the stored data. A detailed description of the encryption technology used as well as

Designation of authorised support and instruction persons: In order to prevent abuse with regard to the administration of your customer account, you can designate up to three dedicated authorised instruction persons within Examiz Services. Only the persons named there may make support enquiries, grant (temporary) account access for Examiz employees and initiate instructions such as deleting the customer account. If no employees are defined, the managing director is deemed to be the person authorised to issue instructions within the meaning of the GDPR by default. The support and instruction authorities can be defined in Examiz within the settings under Support and changed at any time.

Access restriction to client account: Examiz staff do not have access to your customer account. If you wish to contact our Customer Success staff for assistance with the initial set-up of your account or the processing of service requests, it is necessary to release your account to our support staff in advance. Access can only be granted by previously defined support and instruction-authorised persons in the settings under Support and can be deactivated again at any time.

Telephone PIN against social engineering: Should support and instruction persons not be identifiable, e.g. in the case of a support request, our support staff are encouraged to query the currently valid support PIN. This provides additional protection to ensure that information cannot be inadvertently passed on to unauthorised callers. The support PIN can be found by support and instruction staff within

your personal settings in the Support section. You can change the PIN at any time, e.g., if you suspect that the PIN has been compromised.

Increased password security: We increase the security requirements for passwords that you and your employees can assign for your own Examiz account.

l. Data breach notification (Art. 33/34 GDPR)

In the event of a breach of the protection of personal data, reporting obligations to the supervisory authority must be fulfilled and the responsible body as well as the data subjects must be notified. For this purpose, we have set up appropriate notification processes and documented the reporting channels.

Finally, we would like to refer to our website at https://www.examiz.com/privacy-policy/, where you can view or request further information and documents on the topic. Should any questions remain unanswered, please do not hesitate to contact dataprotection@examiz.com.

C. DATA PROTECTION POLICY

a. Statement

The purpose of this data protection policy is to ensure an adequate level of protection of the personal data processed by *Examiz Ltd.*.

b. Definitions

- The information used to identify the data subject is considered as personal data.
- Data protection refers to the process of protecting the personal data that the organization collects and processes, as well as the identity of the data subjects.

c. Scope and application

- This policy applies to all data subjects, data controllers, data processors, and personal data that fall under the responsibility of *Examiz Ltd.*.
- It is up to the data controller and the data protection officer to ensure compliance with this policy and to take the necessary measures to apply it.

d. Objectives

- Clarify the organization's data protection and security strategy
- Ensure the protection of relevant information and critical actions from potential threats
- Ensure that, in case of a system error or any other data protection threat, all the relevant personal data and critical assets maintain a satisfactory level of confidentiality, integrity, and availability, as determined by the top management
- Establish a culture of data protection within the organization

e. Policy

- The policy must be approved by *Examiz Ltd.'* top management.
- All of *Examiz Ltd.'* personal data, including data stored on computers, transmitted over networks, printed, or written on paper, sent by fax, stored on drives and USBs, or transmitted verbally in conversations or over the phone, must be protected from any threat, be it internal, external, deliberate, or accidental.
- Technical measures, such as generalizing the data with anonymity or replacing personal data with random characters, saving the decryption keys in a cold storage device, and adding noise to the data, must be properly applied.
- Any authorization for access to personal data given to a *Examiz Ltd.* employee must be defined and approved by the employee's supervisor.
- The integrity of information must be maintained, and its exactness and completeness must be ensured by protecting it against unauthorized changes and access.
- The confidentiality of information must be ensured. Data must be protected to ensure that valuable or sensitive information is protected against unauthorized disclosures or interruptions.

- *Examiz Ltd.* must train its employees on data protection by putting in place an awareness program on the importance of data protection and ensuring the participation of all staff members.
- The Chief Technology Officer of *Examiz Ltd.* shall create a detailed log file of every change that occurs in the organization's physical infrastructure or infrastructure -as-a-service.
- Real or suspected data protection breaches must be evaluated and reported to the competent authorities.
- Adequate access controls must be put in place and information must be protected against unauthorized access and processing.
- All staff members and contracted external personnel are responsible for adhering to the data protection policy.

D. RECORDS OF PROCESSING ACTIVITIES

a. Talent Data

Processing activity description	
Processing activity name:	Talent data records
Processing creation date:	June 20, 2022
Processing update:	March 12, 2023

Involved parties	Name	Address	ZIP code	City	Country	Phone no.	Email
Data Controller	Nemanja Scepanovic	Kapljevi´ca Marka 43	21000	Novi Sad	Serbia	+381 64320 2431 98 42328	nemanja@examiz.com
Data Protection Officer	n/a	-	-	-	-	-	-

Data processing purpose(s) and types of data		
Main purpose		Provide personality and skill analytics.
Sub-Purpose 1		Find indicators towards behaviour patterns and personality traits based on the collected peer-feedback from nominated reference providers
Sub-Purpose 2		Collect relevant documents to facilitate recruitment and talent development efforts of the customers
Sub-Purpose 3		Track milestones during the selection / hiring process and collect other statistics
Sub-Purpose 4		Fraud detection
Collected Data Type	**Description**	**Data Retention**
Identity	Identity data are provided by the subscribers/users of the Examiz Services. They are required to obtain the consent of data subjects as part of the Examiz Terms & Conditions. • Title/Gender • First name • Last name • Email address • Phone number • Street Address, City and Country • ID Photo	Data will be deleted/ pseudonymised as defined by customer, latest 18 months after creation of an analysis request
Connection data	• IP address • Browser type • Operating system	Data will be deleted/ pseudonymised as defined by customer, latest 18 months after creation of an analysis request
Documents	• Resume • Curriculum Vitae • Cover Letters • Certificates • Transcripts	Data will be deleted/ pseudonymised as defined by customer, latest 18 months after creation of an analysis request

Data Sharing Purpose(s)	Recipient Type	Recipient	Links to related documents
The personal data will only be shared with the users of the Examiz Services within the scope of the respective contract or assessment request. The data are limited to the provided identity information and documents.	Customer	Managers of the analytics or search request	https://www.examiz.com/wp-content/uploads/2020/10/Examiz-Service-Terms-Conditions_03_October_2020.pdf https://www.examiz.com/wp-content/uploads/2020/10/Examiz-User-Agreement_03_October_2020.pdf

Transfers outside the EU	Receiver	Country	Links to related documents
The personal data will not be transferred to countries outside the EU.	n/a	n/a	n/a

Security Measures	Technical	Organizational
	All personal data are permanently encrypted as part of the complete database encryption (AES 256) and access control is being used to protect them from unauthorized access.	Access to encryption keys to database are limited to Examiz administrators.
	Personal data are stored in servers (infrastructure-as-a-service) for a maximum of 18 months. After this period, all personal data are pseudonymised.	Records and logs of pseudonymised are periodically reviewed. Reports on data breaches of used services are continuously monitored. In case of a reported/publicized data breach

		of external providers, Examiz data subjects will be informed in case they are impacted. The data subject may limit the sharing of documents and photos.

b. Reference Provider Data

Processing activity description	
Processing activity name:	Reference provider data records
Processing creation date:	June 20, 2020
Processing update:	March 12, 2021

Involved parties	Name	Address	ZIP code	City	Country	Phone no.	Email
Data Controller	Nemanja Scepanovic	Kapljevi´ca Marka 43	21000	Novi Sad	Serbia	+381 64320 2431 98 42328	nemanja@examiz.com
Data Protection Officer	n/a	-	-	-	-	-	-

Data processing purpose(s) and types of data		
Main purpose		Approach and interview references through an online survey.
Sub-Purpose 1		Offer additional Examiz services
Sub-Purpose 2		Collect statistics on user behaviour
Sub-Purpose 3		Fraud detection
Collected Data Type	**Description**	**Data Retention**
Identity	Identity data are provided by the subscribers/users of the Examiz Services. They are required to obtain the consent of data subjects as part of the Examiz Terms &	Data will be deleted/ pseudonymised as defined by customer, latest 18 months after creation of an analysis request

	Conditions. • Title/Gender • First name • Last name • Email address	
Connection data	• IP address • Browser type • Operating system	Data will be deleted/ pseudonymised as defined by customer, latest 18 months after creation of an analysis request

Data Sharing Purpose(s)	Recipient Type	Recipient	Links to related documents
The personal data will NOT be shared with external parties.	n/a	n/a	https://www.examiz.com/wp-content/uploads/2020/10/Examiz-Service-Terms-Conditions_03_October_2020.pdf https://www.examiz.com/wp-content/uploads/2020/10/Examiz-User-Agreement_03_October_2020.pdf

Transfers outside the EU	Receiver	Country	Links to related documents
The personal data will not be transferred to countries outside the EU.	n/a	n/a	n/a

Security Measures	Technical	Organizational
	All personal data are permanently encrypted as part of the complete database encryption (AES 256) and access control is being used to protect them from unauthorized access.	Access to encryption keys to database are limited to Examiz administrators.
	Personal data are stored in servers (infrastructure-as-a-service) for a maximum of 18 months. After this period, all personal data are pseudonymised.	Records and logs of pseudonymised are periodically reviewed.

c. Customer & Contract Data

Processing activity description	
Processing activity name:	Customer data records
Processing creation date:	June 20, 2020
Processing update:	March 12, 2021

Involved parties	Name	Address	ZIP code	City	Country	Phone no.	Email
Data Controller	Nemanja Scepanovic	Kapljevi´ca Marka 43	21000	Novi Sad	Serbia	+381 64320 2431 98 42328	nemanja@examiz.com
Data Protection Officer	n/a	-	-	-	-	-	-

Data processing purpose(s) and types of data		
Main purpose		Establish and manage service contracts and user accounts.
Sub-Purpose 1		Generate and send invoices
Sub-Purpose 2		Maintain correspondence with subscribers and users to improve the Examiz Services
Sub-Purpose 3		Respond to tickets and user recommendations
Sub-Purpose 4		Fraud detection
Collected Data Type	**Description**	**Data Retention**
Identity	Identity data are provided by the subscribers/users of the Examiz Services. They are required to	Data will be deleted/ pseudonymised latest 30 days after the contract has been terminated.

	obtain the consent of data subjects as part of the Examiz Terms & Conditions. • Title/Gender • First name • Last name • Email address • Phone number • (corporate) Street Address, City and Country	Financial and legal records will be kept as required by the applicable national law.
Connection data	• IP address • Usage data • Browser type • Operating system	Data will be deleted/ pseudonymised latest 30 days after the contract has been terminated. Financial and legal records will be kept as required by the applicable national law.
Documents	• Contracts • Invoices • Business Correspondence	Data will be deleted/ pseudonymised latest 30 days after the contract has been terminated. Financial and legal records will be kept as required by the applicable national law.

Data Sharing Purpose(s)	Recipient Type	Recipient	Links to related documents
The personal data will only be shared with the respective contract partners of the Examiz Services. The data are limited to the provided identity information and documents.	Customer	Customer contract manager and accounting team	https://www.examiz.com/wp-content/uploads/2020/10/Examiz-Service-Terms-Conditions_03_October_2020.pdf https://www.examiz.com/wp-content/uploads/2020/10/Examiz-User-Agreement_03_October_2020.pdf

Transfers outside the EU	Receiver	Country	Links to related documents
The personal data will not be transferred to countries outside the EU.	n/a	n/a	n/a

Security Measures	Technical	Organizational
	All personal data are permanently encrypted as part of the complete database encryption (AES 256) and access control is being used to protect them from unauthorized access.	Access to encryption keys to database are limited to Examiz administrators.
	Personal data are stored in servers (infrastructure-as-a-service) as defined as the data retention. After this period, all personal data are pseudonymised.	Records and logs of pseudonymised are periodically reviewed.
	Personal data managed outside the core Examiz system will be managed exclusively	External tools are reviewed towards if they declare themselves to be GDPR compliant.

	through services that are GDPR compliant	Reports on data breaches of used services are continuously monitored. In case of a reported/publicized data breach of external providers, Examiz data subjects will be informed in case they are impacted.

E. Personal data breach notification form

1. Identification of the data controller

This information is exclusively available to the relevant Data Protection Authority and should not be shared with third parties.

1.1 Organization details	
Organization type: ☐ Private ☐ Public	
Organization name:	
Address:	Postal code:
City:	Country:
1.2 Contact of the data protection officer (to obtain corresponding information)	
Name:	
Address:	Postal code:
City:	Country:
Email:	
Phone number(s):	
1.3 Type of notification	
☐ Complete notification (Sections 2 and 3 shall be completed within 72 h. after becoming aware of the data breach)	
☐ Two-step notification (Section 2 shall be completed within 72 h. after becoming aware of the data breach, while Section 3 shall be completed within four weeks after becoming aware of the data breach)	

2. PRINCIPAL INFORMATION ON DATA BREACH

Under the GDPR (General Data Protection Regulation), Ireland-based organisations must report data breaches to the DPC (Data Protection Commission) within 72 hours of becoming aware of them to be filed online with the DPC (https://forms.dataprotection.ie/report-a-breach-of-personal-data).

2.1 Nature of the data breach
☐ Hacking attack
☐ Phishing attack
☐ Malware
☐ Improper disposal of personal data
☐ Paper lost, stolen, or left in an insecure location
☐ Unauthorized disclosure
☐ Improper written communication (mail, email, fax, phone)
☐ Improper verbal communication
☐ Unauthorized access
☐ Lost or stolen device
☐ Other (please specify):
2.2 Type of the data breach
☐ Breach of confidentiality

☐ Breach of integrity
☐ Breach of availability
2.3 Organization's size — number of employees
☐ 1-9
☒ 10-49
☐ 50-249
☐ 250-749
☐ 750-1000
☐ > 1000
2.4 Organization's size – turnover
☒ ≤ € 2 million
☐ ≤ € 10 million
☐ ≤ € 50 million
☐ > € 50 million
2.5 State where the organization has its main establishment
Specify the country: REPUBLIC OF IRELAND
2.6 Member state where the breach took place

Specify the country: REPUBLIC OF IRELAND (Server infrastructure at Maastricht, Netherlands)				
2.7 Date/time of the breach				
Hour:	**Minute:**	**Day:**	**Month:**	**Year:**
2.8 Date/time of detection				
Hour:	**Minute:**	**Day:**	**Month:**	**Year:**
2.9 What caused the breach? (refer to Q8 in Section 3 if you are not aware of the cause)				
☐ Malicious Attack ☐ Internal ☐ External				
☐ Accident (system failure):				
☐ Negligence (human error):				
☐ Other (please specify):				
2.10 If the breach is a result of a malicious attack, what malicious attack caused the breach?				
☐ Trojans				
☐ Crypto locker				
☐ Distributed denial of service (DoS)				
☐ Malware				
☐ CEO fraud				

☐ Blackmailing
☐ Other (please specify):
2.11 What is/are the likely consequence(s) of this breach?
☐ Data publication
☐ Data theft
☐ Identity theft or fraud
☐ Loss of data
☐ Loss of personal data confidentiality
☐ Property damage
☐ Direct financial loss
☐ Business interruption
☐ Liability issues
☐ Reputational damage
☐ Other (please specify):
2.12 What is the type of data affected/exploited/stolen?
☐ Personal ☐ Sensitive (e.g., health/genetic data) ☐ Non-sensitive

2.13 If the data are personal, what is the encryption status of the data?
☐ Full
☐ Partial
☐ None
2.14 Were the breached data subject to a data protection impact assessment?
☐ Yes
☐ No
2.15 What type of IT support does the organization have?
☐ Internal
☐ External
2.16 What measures have been taken to mitigate the negative effects of the data breach?
☐ Data recovery
☐ Erasure of malware or negative software
☐ Replacement of destroyed property
☐ External testing (i.e., ethical hackers, pen tests, etc.)
☐ Enhancement of data security measures
☐ Other (please specify):

2.17 About the data subject
☐ Customer
☐ User
☐ Employee
☐ Patient
☐ Student
☐ Subscriber
☐ Other (please specify):

3. Complementary information

To be filled out and shared with the Data protection Authority maximum four weeks after becoming made aware of the data breach.

3.1 Date/time of when the attack ended				
Hour:	**Minute:**	**Day:**	**Month:**	**Year:**
3.2 Estimated financial damage				
3.3 How many personal datasets were affected/exploited/stolen?				
3.4 Have the data subjects been notified of the data breach?				
☒ Yes Date:				
☐ No				

3.5 How many data subjects have been notified?	
3.6 Estimated financial damage	
Cost of notification:	**Financial damage:**
3.7 Did the organization take any corrective measures to prevent this exploit from happening again?	
☐ Improvement of data security measures and in particular: ☐ Audit and redesign of data collection procedures ☐ Audit and redesign of data processing procedures ☐ Audit and re-evaluation of the data processor, if applicable ☐ Encryption of data at rest ☐ No data security measures were taken ☐ Other (please specify):	
3.8 What was the cause of the data breach?	
☐ Malicious attack ☐ Internal ☐ External ☐ Accident (system failure) ☐ Negligence (human error) ☐ Other (please specify):	
3.9 If known, what was the motivation or reason behind this data breach (in case of a malicious attack)?	
3.10 If known, what exploit software was used (in case of a malicious attack)?	
☐ Malware ☐ Ransomware ☐ Phishing ☐ SQL injection ☐ Cross-site scripting (XSS)	

☐ Denial of Service (Dos) ☐ Other (please specify):

F. Annex

Data Protection Policy
for EXAMIZ Employees, Workers and Consultants

1 Overview

1.1 The Company takes the security and privacy of your data seriously. We need to gather and use information or 'data' about you as part of our business and to manage our relationship with you. We intend to comply with our legal obligations under the **Data Protection Act 2018** (the '2018 Act') and the **EU General Data Protection Regulation** ('GDPR') in respect of data privacy and security. We have a duty to notify you of the information contained in this policy.

1.2 This policy applies to current and former employees, workers, volunteers, apprentices and consultants. If you fall into one of these categories then you are a 'data subject' for the purposes of this policy. You should read this policy alongside your contract of employment (or contract for services) and any other notice we issue to you from time to time in relation to your data.

1.3 The Company has separate policies and privacy notices in place in respect of job applicants, customers, suppliers and other categories of data subject. A copy of these can be obtained from https://www.examiz.com/privacy-policy/.

1.4 The Company has measures in place to protect the security of your data in accordance with our Data Security Policy. A copy of this can be obtained from [insert name].

1.5 The company will hold data in accordance with our Data Retention Policy. A copy of this can be obtained from [insert name]. We will only hold data for as long as necessary for the purposes for which we collected it.

1.6 The Company is a '**data controller**' for the purposes of your personal data. This means that we determine the purpose and means of the processing of your personal data.

1.7 This policy explains how the Company will hold and process your information. It explains your rights as a data subject. It also explains your obligations when obtaining, handling, processing or storing personal data in the course of working for, or on behalf of, the Company.

1.8 This policy does not form part of your contract of employment (or contract for services if relevant) and can be amended by the Company at any time. It is intended that this policy is fully compliant

with the 2018 Act and the GDPR. If any conflict arises between those laws and this policy, the Company intends to comply with the 2018 Act and the GDPR.

2 Data Protection Principles

2.1 Personal data must be processed in accordance with six '**Data Protection Principles**.' It must:

- be processed fairly, lawfully and transparently;
- be collected and processed only for specified, explicit and legitimate purposes;
- be adequate, relevant and limited to what is necessary for the purposes for which it is processed;
- be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay;
- not be kept for longer than is necessary for the purposes for which it is processed; and
- be processed securely.

We are accountable for these principles and must be able to show that we are compliant.

3 How we define personal data

3.1 '**Personal data**' means information which relates to a living person who can be **identified** from that data (a '**data subject**') on its own, or when taken together with other information which is likely to come into our possession. It includes any expression of opinion about the person and an indication of the intentions of us or others, in respect of that person. It does not include anonymised data.

3.2 This policy applies to all personal data whether it is stored electronically, on paper or on other materials.

3.3 This personal data might be provided to us by you, or someone else (such as a former employer, your doctor, or a credit reference agency), or it could be created by us. It could be provided or created during the recruitment process or during the course of the contract of employment (or services) or after its termination. It could be created by your manager or other colleagues.

3.4 We will collect and use the following types of personal data about you:

- recruitment information such as your application form and CV, references, qualifications and membership of any professional bodies and details of any pre-employment assessments;

- your contact details and date of birth;

- the contact details for your emergency contacts;
- your gender;
- your marital status and family details;
- information about your contract of employment (or services) including start and end dates of employment, role and location, working hours, details of promotion, salary (including details of previous remuneration), pension, benefits and holiday entitlement;
- your bank details and information in relation to your tax status including your national insurance number;
- your identification documents including passport and driving licence and information in relation to your immigration status and right to work for us;
- information relating to disciplinary or grievance investigations and proceedings involving you (whether or not you were the main subject of those proceedings);
- information relating to your performance and behaviour at work;
- training records;
- electronic information in relation to your use of IT systems/swipe cards/telephone systems;
- your images (whether captured on CCTV, by photograph or video); and
- any other category of personal data which we may notify you of from time to time.

4 How we define special categories of personal data

4.1 '**Special categories of personal data**' are types of personal data consisting of information as to:

- your racial or ethnic origin;
- your political opinions;
- your religious or philosophical beliefs;
- your trade union membership;
- your genetic or biometric data;

- your health;
- your sex life and sexual orientation; and
- any criminal convictions and offences.

We may hold and use any of these special categories of your personal data in accordance with the law.

5 How we define processing

5.1 **'Processing'** means any operation which is performed on personal data such as:

- collection, recording, organisation, structuring or storage;
- adaption or alteration;
- retrieval, consultation or use;
- disclosure by transmission, dissemination or otherwise making available;
- alignment or combination; and
- restriction, destruction or erasure.

This includes processing personal data which forms part of a filing system and any automated processing.

6 How will we process your personal data?

6.1 The Company will process your personal data (including special categories of personal data) in accordance with our obligations under the 2018 Act.

6.2 We will use your personal data for:

- performing the contract of employment (or services) between us;
- complying with any legal obligation; or

- if it is necessary for our legitimate interests (or for the legitimate interests of someone else). However, we can only do this if your interests and rights do not override ours (or theirs). You have the right to challenge our legitimate interests and request that we stop this processing. See details of your rights in section 12 below.

We can process your personal data for these purposes without your knowledge or consent. We will not use your personal data for an unrelated purpose without telling you about it and the legal basis that we intend to rely on for processing it.

If you choose not to provide us with certain personal data, you should be aware that we may not be able to carry out certain parts of the contract between us. For example, if you do not provide us with your bank account details, we may not be able to pay you. It might also stop us from complying with certain legal obligations and duties which we have such as to pay the right amount of tax to HMRC or to make reasonable adjustments in relation to any disability you may suffer from.

7 Examples of when we might process your personal data

7.1 We have to process your personal data in various situations during your recruitment, employment (or engagement) and even following termination of your employment (or engagement).

7.2 For example (and see section 7.6 below for the meaning of the asterisks):

- to decide whether to employ (or engage) you;
- to decide how much to pay you, and the other terms of your contract with us;
- to check you have the legal right to work for us;
- to carry out the contract between us including where relevant, its termination;
- training you and reviewing your performance*;
- to decide whether to promote you;
- to decide whether and how to manage your performance, absence or conduct*;
- to carry out a disciplinary or grievance investigation or procedure in relation to you or someone else;

- to determine whether we need to make reasonable adjustments to your workplace or role because of your disability*;
- to monitor diversity and equal opportunities*;
- to monitor and protect the security (including network security) of the Company, of you, our other staff, customers and others;
- to monitor and protect the health and safety of you, our other staff, customers and third parties*;
- to pay you and provide pension and other benefits in accordance with the contract between us*;
- paying tax and national insurance;
- to provide a reference upon request from another employer;
- to pay trade union subscriptions*;
- monitoring compliance by you, us and others with our policies and our contractual obligations*;
- to comply with employment law, immigration law, health and safety law, tax law and other laws which affect us*;
- to answer questions from insurers in respect of any insurance policies which relate to you*;
- running our business and planning for the future;
- the prevention and detection of fraud or other criminal offences;
- to defend the Company in respect of any investigation or litigation and to comply with any court or tribunal orders for disclosure*; and
- for any other reason which we may notify you of from time to time.

7.3 We will only process special categories of your personal data (see above) in certain situations in accordance with the law. For example, we can do so if we have your explicit consent. If we asked for your consent to process a special category of personal data then we would explain the reasons

for our request. You do not need to consent and can withdraw consent later if you choose by contacting [insert].

7.4 We do not need your consent to process special categories of your personal data when we are processing it for the following purposes, which we may do:

- where it is necessary for carrying out rights and obligations under employment law;
- where it is necessary to protect your vital interests or those of another person where you/they are physically or legally incapable of giving consent;
- where you have made the data public;
- where processing is necessary for the establishment, exercise or defence of legal claims; and
- where processing is necessary for the purposes of occupational medicine or for the assessment of your working capacity.

7.5 We might process special categories of your personal data for the purposes in paragraph 7.2 above which have an asterisk beside them. In particular, we will use information in relation to:

- your race, ethnic origin, religion, sexual orientation or gender to monitor equal opportunities;
- your sickness absence, health and medical conditions to monitor your absence, assess your fitness for work, to pay you benefits, to comply with our legal obligations under employment law including to make reasonable adjustments and to look after your health and safety; and
- your trade union membership to pay any subscriptions and to comply with our legal obligations in respect of trade union members.

7.6 While we might use analytics tools to prepare informed decisions, we do not take automated decisions about you using your personal data or use profiling in relation to you.

8 Sharing your personal data

8.1 Sometimes we might share your personal data with group companies or our contractors and agents to carry out our obligations under our contract with you or for our legitimate interests.

8.2 We require those companies to keep your personal data confidential and secure and to protect it in accordance with the law and our policies. They are only permitted to process your data for the lawful purpose for which it has been shared and in accordance with our instructions.

8.3 Your personal data might be shared with external service providers such as payroll and tax services.

8.4 For EU citizens: We do not send your personal data outside the European Economic Area. Our servers including backups are located in the EU, currently in Amsterdam, The Netherlands. If this changes you will be notified of this and the protections which are in place to protect the security of your data will be explained.

9 How should you process personal data for the Company?

9.1 Everyone who works for, or on behalf of, the Company has some responsibility for ensuring data is collected, stored and handled appropriately, in line with this policy and the Company's Data Security and Data Retention policies.

9.2 The tasks of the Company's Data Protection Officer/Data Protection Manager **are assumed by the Chief Technology Officer** is responsible for reviewing this policy and updating the Board of Directors on the Company's data protection responsibilities and any risks in relation to the processing of data. You should direct any questions in relation to this policy or data protection to this person.

9.3 You should only access personal data covered by this policy if you need it for the work you do for, or on behalf of the Company and only if you are authorised to do so. You should only use the data for the specified lawful purpose for which it was obtained.

9.4 You should not share personal data informally.

9.5 You should keep personal data secure and not share it with unauthorised people.

9.6 You should regularly review and update personal data which you have to deal with for work. This includes telling us if your own contact details change.

9.7 You should not make unnecessary copies of personal data and should keep and dispose of any copies securely.

9.8 You should use strong passwords.

9.9 You should lock your computer screens when not at your desk.

9.10 Personal data should be encrypted before being transferred electronically to authorised external contacts.

9.11 Consider anonymising data or using separate keys/codes so that the data subject cannot be identified.

9.12 Do not save personal data to your own personal computers or other devices.

9.13 Personal data should never be transferred outside the European Economic Area except in compliance with the law and authorisation of the Data Protection Officer or Chief Technology Officer.

9.14 You should lock drawers and filing cabinets. Do not leave paper with personal data lying about.

9.15 You should not take personal data away from Company's premises without authorisation from your line manager or Data Protection Officer.

9.16 Personal data should be shredded and disposed of securely when you have finished with it.

9.17 You should ask for help from our Data Protection Officer/Data Protection Manager if you are unsure about data protection or if you notice any areas of data protection or security we can improve upon.

9.18 Any deliberate or negligent breach of this policy by you may result in disciplinary action being taken against you in accordance with our disciplinary procedure.

9.19 It is a criminal offence to conceal or destroy personal data which is part of a subject access request (see below). This conduct would also amount to gross misconduct under our disciplinary procedure, which could result in your dismissal.

9.20 Any deliberate or negligent breach disclosure of access credentials such as user names or passwords may result in disciplinary action being taken against you in accordance with our disciplinary procedure, as well the pursuit of legal actions and claims regarding suffered damages and losses.

10 How to deal with data breaches

10.1 We have robust measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur (whether in respect of you or someone else) then we must take notes and keep evidence of that breach. If the breach is likely to result in a risk to the rights

and freedoms of individuals then we must also notify the Data Protection Commission's Office within 72 hours.

10.2 If you are aware of a data breach you must contact [insert name] immediately and keep any evidence you have in relation to the breach.

11 Subject access requests

11.1 Data subjects can make a '**subject access request**' ('SAR') to find out the information we hold about them. This request must be made in writing. If you receive such a request you should forward it immediately to the Data Protection Officer/Data Protection Manager who will coordinate a response.

11.2 If you would like to make a SAR in relation to your own personal data you should make this in writing to [insert name]. We must respond within one month unless the request is complex or numerous in which case the period in which we must respond can be extended by a further two months.

11.3 There is no fee for making a SAR. However, if your request is manifestly unfounded or excessive we may charge a reasonable administrative fee or refuse to respond to your request.

12 Your data subject rights

12.1 You have the right to information about what personal data we process, how and on what basis as set out in this policy.

12.2 You have the right to access your own personal data by way of a subject access request (see above).

12.3 You can correct any inaccuracies in your personal data. To do you should contact [insert name].

12.4 You have the right to request that we erase your personal data where we were not entitled under the law to process it or it is no longer necessary to process it for the purpose it was collected. To do so you should contact [insert name].

12.5 While you are requesting that your personal data is corrected or erased or are contesting the lawfulness of our processing, you can apply for its use to be restricted while the application is made. To do so you should contact [insert name].

12.6 You have the right to object to data processing where we are relying on a legitimate interest to do so and you think that your rights and interests outweigh our own and you wish us to stop.

12.7 You have the right to object if we process your personal data for the purposes of direct marketing.

12.8 You have the right to receive a copy of your personal data and to transfer your personal data to another data controller. We will not charge for this and will in most cases aim to do this within one month.

12.9 With some exceptions, you have the right not to be subjected to automated decision-making.

12.10 You have the right to be notified of a data security breach concerning your personal data.

12.11 In most situations we will not rely on your consent as a lawful ground to process your data. If we do however request your consent to the processing of your personal data for a specific purpose, you have the right not to consent or to withdraw your consent later. To withdraw your consent, you should contact [insert name].

12.12 You have the right to complain to the Data Protection Commission. The Data Protection Commission (DPC) is the Irish national independent authority responsible for upholding the fundamental right of individuals in the EU to have their personal data protected.

The DPC is the Irish supervisory authority for the General Data Protection Regulation (GDPR), and also has functions and powers related to other important regulatory frameworks including the Irish ePrivacy Regulations (2011) and the EU Directive known as the Law Enforcement Directive. Full contact details including a helpline number can be found on the Data Protection Commission's Office website (https://www.dataprotection.ie/). This website has further information on your rights and our obligations.