VERŻJONI ELETTRONIKA

Suppliment tal-Gazzetta tal-Gvern ta' Malta Nru. 21,644, 15 ta' Mejju, 2026
Taqsima B

L.N. 151 of 2026

COMPANIES ACT
(CAP. 386)

Companies Act (Central Data Repository) Regulations, 2026

IN EXERCISE of the powers conferred by article 425(1)(q) of the Companies Act, the Minister responsible for the registration of commercial partnerships has made the following regulations:-

Citation, scope and commencement.

1. (1) The title of these regulations is the Companies Act (Central Data Repository) Regulations, 2026.

(2) The scope of these regulations is to prescribe and provide the necessary requirements and qualifications in relation to the establishment, administration and upkeep of the central data repository.

(3) These regulations shall come into force on such date or dates as the Minister responsible for the registration of commercial partnerships may by notice in the Gazette establish and different dates may be so established for different provisions and, or purposes of these regulations.

PART I
PRELIMINARY PROVISIONS

Interpretation.

2. (1) In these regulations, unless the context otherwise requires:

"Act" means the Companies Act; Cap. 386.

"APIs" means the Application Programme Interfaces;

"beneficial owner" shall have the same meaning as assigned to it in the Prevention of Money Laundering and Funding of Terrorism Regulations; S.L. 373.01.

"biometric data" means the personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of such natural person, such as facial images or dactyloscopic data;

"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;

S.L. 373.01.

"competent authority" shall have the same meaning as assigned to it in the Prevention of Money Laundering and Funding of Terrorism Regulations;

Cap. 258.

"identity document" means a legally valid identity document as provided in the Identity Card and other Identity Documents Act;

"identifiable natural person" means a person who 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 to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of such natural person;

"personal data" means any information relating to an identified or identifiable natural person and the said person is known as the "data subject";

"processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether by automated means or otherwise, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

"Registrar" means the person appointed by the Minister pursuant to article 400 of the Act;

"Regulation (EU) 2016/679" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC;

"relying party" shall have the same meaning as assigned to it in regulation 7;

"repository" means the central data repository established by regulation 3;

S.L. 373.01.

"subject person" shall have the same meaning as assigned to it in the Prevention of Money Laundering and Funding of Terrorism Regulations;

VERŻJONI ELETTRONIKA

"user" shall have the same meaning as assigned to it in regulation 6.

(2) Unless the context otherwise requires, words and phrases used in these regulations which are not defined herein, shall have the same meaning as assigned to them in the Act.

PART II
SCOPE OF THE REPOSITORY AND DUTIES OF THE REGISTRAR

Establishment of the repository.

3. (1) The Registrar shall establish, manage and administer a secure digital repository in accordance with these regulations.

(2) The repository shall serve as a digital mechanism through which a user may make available data and information relating to himself and, or to his involvement in a body corporate, for the purpose of access and use by a relying party in the discharge of its duties and functions under applicable laws, subject to any limitations established in these regulations.

Functions of the repository.

4. (1) The repository shall enable a user, subject to any procedures as may be established by the Registrar, or any limitation imposed by these regulations to:

(a) securely upload, submit, store, retrieve, rectify, erase, and present data and information which a user elects to make available within the repository for the purpose of enabling a relying party to access, use or otherwise process such data and information for specific purposes;

(b) under the control of a user, and in accordance with the user's right of selective disclosure as prescribed under these regulations, make available information in a digital form to a relying party in a secure and verifiable manner which ensures the integrity and authenticity of such data and information;

(c) communicate with relying parties through the repository for the purpose of providing such with supplementary data or clarifications;

(d) generate and compile, by means facilitated through the repository, reports derived from the data and information related to the user, and to make available such reports to a relying party in accordance with these regulations;

(e) access a log of all actions carried out by the user within the repository, including a list of each relying party to

which the user has elected to make available data, information and reports, and where applicable, the data, information and reports that were made available to each specific relying party; and

(f) carry out such other actions as may be necessary for the proper implementation of these regulations and the attainment of the purposes of the repository, in accordance with these regulations, as may be determined by the Registrar.

(2) The repository shall enable relying parties, subject to the user's selective disclosure under these regulations to:

(a) request, obtain, collect and receive data, information and reports made available through the repository by users;

(b) access and process such data, information and reports for the purpose of enabling the relying party to perform its duties and functions under any applicable laws;

(c) retain a log, in accordance with any procedures as may be established by the Registrar, of the data, information and reports received or accessed by them through the repository;

(d) communicate with users and other relying parties through the repository for the purpose of requesting supplementary data or clarifications; and

(e) carry out such other actions as may be necessary for the proper implementation of these regulations and the attainment of the purposes of the repository in accordance with the regulations, as may be prescribed by the Registrar.

Voluntary use of the repository.

(3) The use of the repository by users and relying parties shall be voluntary and shall not:

(a) be interpreted to constitute a mandatory means for the uploading, submission, storage, requesting or receipt of data and information;

(b) preclude or restrict the submission, provision or receipt of such data and information by any other lawful means;

(c) give rise to any presumption that a relying party is required to request or obtain data and information exclusively through the repository; or

(d) affect the validity, admissibility or legal effect of any

VERŻJONI ELETTRONIKA

data and information exchanged in any manner outside the repository by any other lawful means.

(4) These regulations shall not be construed as limiting the rights and obligations of a relying party to conduct due diligence, verification or information requests by means other than the repository, in accordance with the Prevention of Money Laundering Act and its subsidiary regulations. Cap. 373.

Duties of the Registrar.

5. (1) It shall be the sole duty of the Registrar, in accordance with article 401(1) of the Act to establish, manage, operate, and maintain the repository in accordance with these regulations. The Registrar shall exercise all such powers and perform all duties as may be necessary to ensure the proper functioning of the repository.

Data retention period.

(2) Any personal data contained in the repository shall be retained for a period of five (5) years following the closure of the account of the user or the termination of the repository, as may be applicable:

Provided that the period of five (5) years may be further extended by the Registrar, up to a maximum retention period of ten (10) years, where such extension is necessary for the purposes of the prevention, detection, analysis, investigation or prosecution of money laundering, associated predicate offences, funding of terrorism or any other serious criminal offence, or any other obligation imposed by law requiring the Registrar to process such personal data.

PART III
USERS, RELYING PARTIES AND FUNCTIONS OF THE REPOSITORY

Users of the repository.

6. (1) The following persons shall, be authorised to access and use the repository as a user in accordance with these regulations, subject to compliance with such registration, verification or accreditation procedures as may be determined by the Registrar:

(a) any officer, judicial representative or legal representative of a company;

(b) any partner in a commercial partnership;

(c) any person who is duly authorised to represent or act on behalf of any other body corporate;

(d) any subject person, acting on behalf of any of the persons referred to in paragraphs (a) to (c), provided that such

S.L. 373.01.

person is duly authorised in accordance with the Prevention of Money Laundering and Funding of Terrorism Regulations; and

(e) any other person as the Registrar may, from time to time publish on a website maintained by him, determine to be eligible to access and use the repository, subject to such conditions as the Registrar may impose.

(2) The Registrar may establish such criteria, conditions, technical requirements and verification procedures as may be necessary to regulate access to, and use of the repository by the users referred to in sub-regulation (1).

Relying parties of the repository.

7. (1) The following shall, subject to undergoing such registration, verification or accreditation process as may be established by the Registrar, be authorised to access and use the repository as a relying party in accordance with these regulations:

(a) any competent authority, insofar as such access is necessary for the performance of their functions and duties;

(b) any subject persons, for the sole purpose of carrying out customer due diligence and related obligations in accordance with the Prevention of Money Laundering Act and its subsidiary regulations; and

Cap. 373.

(c) any other person as the Registrar may, from time to time publish on a website maintained by him. The Registrar may determine persons to be eligible to access and use the repository, subject to such conditions that he may impose.

(2) Access by the relying parties referred to in sub-regulation (1) shall be granted in accordance with these regulations and shall be limited to the extent needed for the performance of the functions and duties in accordance with the purpose referred to in sub-regulation (1), and to what is necessary and proportionate to the objectives pursued.

(3) The relying parties accessing and receiving personal data through the repository shall assume the role of separate controllers and any processing of personal data processed by the relying parties for the purposes specified in sub-regulation (1) shall fully comply with the provisions of Regulation (EU) 2016/679 and the Data Protection Act, including the regulations made thereunder.

Cap. 586.

Access by competent authorities.

8. (1) The data, information and reports held in the repository shall, through the use of APIs or any other technical means, be accessible by any competent authority upon the selective disclosure of the user, in conformity with the procedures established by the

Registrar, who shall access and make use of the data, information and reports contained in the repository on a case-by-case basis and to the extent that this shall be necessary for the prevention, detection, investigation or prosecution of money laundering, associated predicate offences, funding of terrorism or any other serious criminal offence. For the avoidance of any doubt this shall include supporting investigations concerning any such offence, including the identification, tracing and freezing of the assets related to such investigation.

(2) The data, information and reports contained in the repository may also be used to produce such aggregate or statistical data as may be required by the competent authorities for the same purposes as are referred to in sub-regulation (1).

(3) Each competent authority accessing data, information and reports contained in the repository in accordance with these regulations shall:

(a) designate one (1) or more officers or employees that shall have access to the repository, with each designated officer or employee being granted the said rights only upon undergoing such registration or accreditation process, as may be established by the Registrar;

(b) implement the appropriate safeguards to ensure that data, information and reports held in the repository are accessed and used only when required for the purposes established in regulation 7(1);

(c) have due regard to the sensitive nature of the data, information and reports processed:

(i) to ensure that the officers and employees maintain high professional standards of confidentiality and adhere with any applicable data protection law, including through monitoring compliance with the said requirements, and that all their officers and employees are of high integrity;

(ii) to provide any officer or employee designated in terms of sub-regulation (4) or any officer or employee able to request any such employee to use the repository, with the appropriate data protection training covering, in particular, the handling of personal data through the repository in accordance with the applicable data protection law;

(iii) to establish internal policies and procedures establishing the conditions and circumstances in which data, information and reports are to be obtained from the repository, and processed for the purposes specified in regulation 7(1);

(iv) to implement the appropriate technical and organisational measures to ensure the security of the data, information and reports to high technological standards; and

(v) to ensure that the Registrar is promptly informed whenever an officer or employee is no longer to be considered as a designated employee in terms of sub-regulation (3).

(d) whenever the competent authority becomes aware that the data, information or reports held in the repository are not correct or are otherwise not up-to-date, the competent authority concerned shall immediately notify the Registrar;

(e) hold statistical data on the number of requests and the data, information and reports that have been obtained, collected and received by them through the repository, and shall make the same available to the Registrar.

(4) Any data, information or reports obtained through the repository shall be kept confidential by the competent authorities and by their officers, employees or agents, past and present, and any use thereof other than for the purposes established in these regulations shall be considered as an unauthorised disclosure of the same:

Provided that competent authorities may, upon a lawful request from another competent authority and where necessary for the prevention, detection, investigation or prosecution of money laundering, associated predicate offences, the funding of terrorism, or any other serious criminal offence, share with such competent authority any data, information and reports obtained through the repository.

Reporting of unauthorised access.

9. In the event that the competent authority, or any other relying party making use of the repository in accordance with these regulations, become aware of any unauthorised disclosure of, or access to, or use of data, information and reports held within the repository, the competent authority or any other relying party shall promptly notify the Registrar and provide him with any information in relation to any such incident as may be requested by the Registrar.

Restriction or suspension of access.

10. Where the Registrar considers that a relying party is not implementing the necessary safeguards against unauthorised or unjustified access to, or use of, the repository and the data and information contained therein, or is otherwise failing to comply with its obligations under these regulations, he may restrict, suspend or terminate access, and only reinstate it once the necessary measures have been implemented to prevent the same from occurring again.

Data and information that may be uploaded.

11. (1) Subject to these regulations, users may securely upload, submit, store, retrieve, rectify, erase, and submit the following data and information on the repository:

(a) an identity document of the user, including all particulars contained therein and any photographic image forming part thereof;

(b) documentary evidence of the user's registered address;

(c) details of any service address provided for the purposes of representation or correspondence, and where applicable, together with the written consent of the person providing such service address;

(d) where applicable, documentary evidence of the engagement or appointment of a subject person acting on behalf of the user in accordance with these regulations; and

(e) such other data and information as may be prescribed by the Registrar from time to time, provided that such data and documentation shall necessarily be collected by relying parties in order to comply with their obligations at law.

(2) The Registrar may, where he deems it necessary for the proper administration of the repository or for the verification of the identity of users, or compliance with applicable law, require users to submit any additional documentation, information or evidence, as he may consider necessary.

No derogation from existing obligations.

Cap. 373.

12. (1) The provision of data and information by users to the Registrar in accordance with these regulations shall not imply that such users do not remain equally obliged to provide any information requested of them by any subject persons taking customer due diligence measures in accordance with the Prevention of Money Laundering Act and applicable regulations.

(2) Subject persons shall not rely on the data, information and reports that are securely uploaded or otherwise submitted by such

subject persons acting on behalf of a user through the repository, to fulfil any of their customer due diligence obligations and any other obligations imposed by them through applicable laws, and shall not exonerate such subject persons from any responsibilities and duties incumbent upon them in terms of such applicable laws.

Processing of personal data by the Registrar.

Cap. 586.

13. (1) Any processing of personal data conducted by the Registrar in its capacity of a controller in terms of Article 4(7) of Regulation (EU) 2016/679, shall fully comply with the provisions of Regulation (EU) 2016/679 and the Data Protection Act, including any regulations made thereunder and the fundamental rights and freedoms of the data subjects.

(2) The Registrar shall be responsible for ensuring the security of the repository, including safeguarding the ongoing confidentiality, integrity and availability of the personal data processed within the repository for the purposes of these regulations.

(3) The Registrar, while taking into account the nature, scope, context and purposes of processing, as well as the risks of varying likelihood and severity for the rights and freedoms of the data subjects, both at the time of the determination of the means for processing as well as at the time of the processing itself, shall implement appropriate technical and organisational measures, in an effective manner and integrate the necessary safeguards into the processing in order to protect the rights of the data subjects and to ensure a level of security appropriate to the risk.

(4) The Registrar shall monitor the effectiveness of the security measures implemented in relation to the repository and take the necessary organisational measures related to self-monitoring and supervision to ensure compliance with the principle of integrity and confidentiality as established in Article 5(1)(f) of Regulation (EU) 2016/679.

(5) The Registrar shall provide its employees with appropriate training covering, in particular, on data security and data protection rules and applicable fundamental rights, before enabling its employees to handle any personal data within the repository.

(6) The Registrar shall ensure that the relying parties with a right to access the repository create profiles describing the functions and responsibilities of the officers or employees who are authorised to access the repository.

(7) The Registrar shall ensure that the relying parties authorised to access the repository have access only to the data

covered by their access authorisation, by means of individual user identities and confidential access modes only.

(8) The data protection officer designated by the Registrar in accordance with Article 37(1)(a) of Regulation (EU) 2016/679, shall be involved and consulted in a timely manner on all matters in relation to the protection of personal data processed within the repository.

(9) For the purposes of ensuring and to be able to demonstrate that the processing of personal data is performed in accordance with the provisions of Regulation (EU) 2016/679, the Registrar shall implement the appropriate data protection policies, which policies shall be periodically reviewed and updated where necessary.

Powers and duties of the Registrar under applicable laws. S.L. 373.01.

14. (1) In the performance of the functions conferred by these regulations, the Malta Business Registry shall act as a supervisory authority within the meaning of the Prevention of Money Laundering and Funding of Terrorism Regulations, and shall exercise such powers and carry out such duties and responsibilities as are assigned to a supervisory authority under the said regulations.

(2) The Registrar shall perform the functions assigned to him under these regulations and under the Companies Act (Register of Beneficial Owners) Regulations. S.L. 386.19.

Verification and authentication.

15. (1) The Registrar shall ensure that all data and information uploaded or transmitted through the repository by a user are subject to electronic verification and validation, in order to ensure the accuracy, authenticity and integrity of such data and information.

(2) For the purposes of sub-regulation (1), the Registrar shall have the power to carry out checks to ensure the verification of the identity of any user who shall request access to the repository, as well as any data and information being uploaded or stored on the repository by such user, including through the use of APIs or any other technical means, such as the use of electronic identification systems, or any other system, insofar as such system operates in accordance with these regulations:

Provided that where any system used for the purpose of this regulation is operated or supplied by a third party, the Registrar shall only rely on the use of such system after it has ascertained that the third party operating or supplying such system shall apply to that processing activity, appropriate technical and organisational measures to ensure an appropriate level of security to the risk posed, and shall integrate the necessary safeguards into the processing, in order to protect the rights and freedoms of data subjects, and that such processing activity shall be carried out in accordance with any obligations incumbent on the Registrar or the third party in accordance with Regulation (EU) 2016/679, as well as any obligations arising from the Data Protection Act including the regulations made thereunder.

Cap. 586.

(3) For the purposes of effectively operating the repository, there may be the processing of biometric data only where such processing is strictly necessary for reasons of substantial public interest, in particular for the prevention of identity fraud, including by ensuring the secure and reliable verification and validation of the identity of users. Such processing shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to protect the fundamental rights and the interests of the data subjects.

(4) The Registrar may, where necessary for the proper implementation and attainment of the purposes of the repository under these regulations request, access, obtain, process and use any information relating to users from public authorities or bodies established by law, and any registries or other repositories administered by the same, and any such public authority or body shall, subject to any procedures established by it, provide the Registrar with such data and information, including through the use of APIs or any other technical means.

Selective disclosure.

16. (1) Subject to the provisions of these regulations, a user shall have the right to determine the relying parties to whom access to the data, information and reports pertaining to him and stored in the repository may be granted.

(2) Subject to the provision of these regulations a user may, at any time and without the need to assign a reason, revoke or vary an authorisation granted by him in accordance with sub-regulation (1), whether in respect of one (1) or more relying parties, and such revocation or variation shall take effect in accordance with such procedures, as may be established by the Registrar.

VERŻJONI ELETTRONIKA

Validity and legal effect of data and information uploaded on the repository.

17. (1) Any data and information uploaded or transmitted through the repository by a user and verified in accordance with these regulations, shall be deemed to constitute a valid copy of such data and information for all intents and purposes of law:

Provided that such data and information shall be duly authenticated in conformity with any procedure as may be established by the Registrar from time to time, including the use of any electronic signatures.

(2) Without prejudice to the generality of the foregoing, any valid copy of data and information uploaded or transmitted in accordance with sub-regulation (1), shall not be denied legal effect on the ground that it is in electronic form.

Monitoring and access logs.

18. The Registrar shall ensure that all data processing operations in the repository are logged for the purposes of checking the security and the lawfulness of the data processing as well as for the purposes of self-monitoring. The Registrar shall, upon request, make the logs of its processing operations available to the Information and Data Protection Commissioner for the purpose of fulfilling his tasks and exercising his powers.

Fees.

19. The Registrar may establish and levy such fees as may be prescribed for access to, and use of the repository, including fees relating to registration, maintenance, access, verification, authentication or any other service provided under these regulations.

PART IV – PENALTIES

Offences and penalties.

20. Any person who voluntarily makes a statement, declaration or otherwise provides to the Registrar, through the repository, information that is misleading, false or deceptive, or makes any other fraudulent use of the repository, shall be guilty of an offence and shall be liable on conviction to a fine (*multa)* of not more than fifty thousand euro (€50,000), or to imprisonment for a term not exceeding three (3) years, or to both such fine (*multa*) and imprisonment.

Ippubblikat mid-Dipartiment tal-Informazzjoni (doi.gov.mt) — Valletta — ***Published by the Department of Information (doi.gov.mt) — Valletta***
Mitbugħ fl-Istamperija tal-Gvern fuq karta FSC — ***Printed at the Government Printing Press on FSC certified paper***

Prezz/*Price*
€0.63