

# User Guidelines

## Companies Act (Central Data Repository) Regulations, 2026

### Purpose

The aim of the Companies Act (Central Data Repository) Regulations, 2026 (the "regulations") include:

- the creation of a secure digital central data repository (the "repository") managed by the Registrar of Companies (the "Registrar") that allows company officers and legal representatives to manage personal and corporate data in a single location;
- assistance to subject persons and competent authorities in discharging their duties under anti-money laundering and counter-funding of terrorism laws;
- the use of advanced technological standards, such as Application Programme Interfaces (APIs) and biometric data, to verify the identity of users and ensure the authenticity of uploaded documents;
- the implementation of the principle of "selective disclosure", ensuring that users retain total control over which specific relying parties can access their information and that the repository remains a tool for convenience rather than a mandatory burden for involved parties;
- assurance that verified electronic data within the repository is deemed a valid copy for all legal purposes and cannot be denied legal effect due to its digital form;
- the elimination of bottlenecks and decreased operational costs by providing a seamless data-sharing mechanism that remains strictly voluntary for all parties;
- positioning the Malta Business Registry as a supervisory authority that ensures all data processing aligns with the Data Protection Act (Chapter 586 of the Laws of Malta) and GDPR (EU Regulation 2016/679).

## Provisions

- **Regulation 1 – Citation, scope and commencement**

Establishes the official title of the regulations and entry into force on such date as the Minister responsible for the registration of commercial partnerships may appoint by notice in the Gazette and different dates may be appointed for different provisions or different purposes of the regulations.

- **Regulation 2 – Interpretation**

Clearly defines the key terms used throughout the regulations for enhanced legal certainty.

- **Regulation 3 – Establishment of the repository**

Mandates that the Registrar shall establish, manage and administer the repository as a digital mechanism through which a user may share data relating to himself or to his involvement in a body corporate in order to be accessed or used by a relying party.

- **Regulation 4 – Functions of the repository; Voluntary use of the repository**

Outlines user capabilities (uploading, storing, and sharing data selectively) and relying party capabilities (requesting and receiving data). Use of the repository is voluntary and does not replace other lawful means of information exchange.

- **Regulation 5 – Duties of the Registrar; Data retention period**

- Details the Registrar's duties to establish, manage, operate and maintain the repository and establishes a five (5) year data retention period extendable to a maximum period of ten (10) years if the data is required for investigating serious crimes, such as money laundering or terrorism financing.

- **Regulation 6 – Users of the repository**

Defines authorised users of the repository, including company officers, partners, and representatives of bodies corporate. It also outlines the Registrar's powers to regulate access to and use of the repository by users.

- **Regulation 7 – Relying parties of the repository**

Defines relying parties who may be authorised to access and use the repository, such as competent authorities and subject persons conducting due diligence. It also defines strict compliance with the GDPR, the Data Protection Act and relevant regulations made thereunder in relation to access to the repository and receipt of data, information and reports.

- **Regulation 8 – Access by competent authorities**

Governs access by competent authorities, requiring them to designate specific officers or employees to access the repository, and to implement safeguards

for data used in investigating financial crimes.

- **Regulation 9 – Reporting of unauthorised access**

Obliges relying parties making use of the repository to promptly inform the Registrar of any unauthorized or unjustified access to the repository.

- **Regulation 10 – Restriction or suspension of access**

Empowers the Registrar to terminate or suspend access to the repository and to any data and information contained therein to any relying party failing to implement the necessary security safeguards and to only reinstate it once the necessary measures have been implemented to prevent the same from occurring again.

- **Regulation 11 – Data and information that may be uploaded**

Lists the specific data and information users may upload, submit, store, retrieve, rectify, erase and submit on the repository, including identity documents, evidence of registered addresses, and documentation of subject person engagement.

- **Regulation 12 – No derogation from existing obligations**

Clarifies that using the repository does not exempt users or subject persons from their existing legal obligations to provide or collect information for customer due diligence purposes in accordance with applicable laws and regulations.

- **Regulation 13 – Processing of personal data by the Registrar**

Designates the Registrar as a “data controller” under GDPR and the Data Protection Act and requires appropriate technical and organizational security measures in order to protect the rights and freedoms of data subjects, mandatory staff training, and enforcement of strict access controls for authorized users. This involves continuous monitoring, consultation with the data protection officer designated by the Registrar, and the regular updating of policies to protect data integrity and subject rights.

- **Regulation 14 – Powers and duties of the Registrar under applicable law**

States that the Malta Business Registry acts as a supervisory authority in terms of the Prevention of Money Laundering and Funding of Terrorism Regulations (S.L. 373.01) and maintains its duties under the Companies Act (Cap. 386).

- **Regulation 15 – Verification and authentication**

Requires the Registrar to verify all data and user identities using secure electronic systems, ensuring third-party providers meet strict data protection standards. Biometric data is permitted only when strictly necessary to prevent identity fraud, and the Registrar may access information from other public authorities to ensure the repository remains accurate and functional.

- **Regulation 16 – Selective disclosure**

Grants users the right to choose which relying parties see their data, information and reports stored in the repository and the right to vary or revoke such access to any one or more relying parties following the procedures established by the Registrar.

- **Regulation 17 – Validity and legal effect of data and information uploaded on the repository**

Mandates that verified and authenticated electronic data and information uploaded or transmitted through the repository by a user constitutes a valid copy for all legal purposes provided they are authenticated in accordance with procedures issued by the Registrar. Valid copy of data and information shall not be denied legal effect on the grounds that they are in electronic form.

- **Regulation 18 – Monitoring and access logs**

Requires the Registrar to maintain logs of all data processing operations to ensure security, lawfulness, and internal oversight. These logs must be provided to the Information and Data Protection Commissioner upon request to assist with their regulatory and supervisory duties.

- **Regulation 19 – Fees**

Authorizes the Registrar to charge fees for access to and use of the repository, including fees relating to registration, maintenance, access and verification services.

- **Regulation 20 – Offences and penalties**

Establishes criminal penalties for providing false or misleading information through the repository, or for making fraudulent use of the repository, including a fine of up to fifty-thousand euro (€50,000) and, or up to three (3) years imprisonment.

## Conclusion

Should more information be required kindly contact the MBR on 22582300 or at [legal.enforcement@mbr.mt](mailto:legal.enforcement@mbr.mt).

***N.B.** The User Guidelines contained within this document is solely intended to serve as guidelines and should not be construed as legislation. This document should not be considered as an exhaustive description of the instrument nor a substitute thereof or a legislative supplement to it. The Guidelines do not purport to be an authoritative ruling on the interpretation of the legislation. Please refer to the related legislation for a more comprehensive understanding.*