SUBSIDIARY LEGISLATION 586.14

ARTIFICIAL INTELLIGENCE (DESIGNATION OF THE INFORMATION AND DATA PROTECTION COMMISSIONER FOR THE PURPOSES OF REGULATION (EU) 2024/1689) REGULATIONS

10th October, 2025*

LEGAL NOTICE 227 of 2025.

Citation, scope and commencement.

1. (1) The title of these regulations is the Artificial Intelligence (Designation of the Information and Data Protection Commissioner for the purposes of Regulation (EU) 2024/1689) Regulations.

(2) The scope of these regulations is to implement the provisions of Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

(3) Regulations 5 to 7 and 9 to 12 shall come into force on the 2nd August 2026.

Interpretation.

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

"Act" means the Data Protection Act; Cap. 586.

"AI system" shall have the same meaning assigned to in Regulation (EU) 2024/1689;

"Commissioner" means the Information and Data Protection Commissioner appointed in accordance with article 11 of the Act; Cap. 586.

"importer" shall have the same meaning assigned to in Regulation (EU) 2024/1689;

"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 (General Data

*Regulations 5 to 7 & 9 to 12 are not in force.

Protection Regulation);

"Regulation (EU) 2024/1689" means Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

(2) Unless the context otherwise requires, words and phrases used in these regulations which are not defined in this regulation shall have the same meaning as is assigned to them in the Act, including regulations made thereunder, Regulation (EU) 2016/679 and Regulation (EU) 2024/1689.

Designation of market surveillance authority.

3. The Commissioner shall be designated as the market surveillance authority for the purpose of Regulation (EU) 2024/1689 for the following high-risk AI systems:

(a) high-risk biometric systems in so far as the systems are used for law enforcement purposes, border management and justice and democracy, where permitted by law, and these shall include:

(i) remote biometric identification systems:

Provided that this shall not include AI systems intended to be used for biometric verification the sole purpose of which is to confirm that a specific natural person is the person he claims to be;

(ii) AI systems intended to be used for biometric categorisation, according to sensitive or protected attributes or characteristics based on the inference of those attributes or characteristics;

(iii) AI systems intended to be used for emotion recognition;

(b) high-risk systems intended to evaluate and classify emergency calls by natural persons or to be used to dispatch, or to establish priority in the dispatching of emergency first response services, including by Police, fire-fighters and medical aid, as well as of emergency healthcare patient triage systems;

(c) high-risk systems used for law enforcement, in so far as their use is permitted by law, and these shall include:

(i) AI systems intended to be used by or on behalf of law enforcement authorities to assess the risk of a natural person becoming the victim of criminal offences;

(ii) AI systems intended to be used by or on behalf of law enforcement authorities as polygraphs or similar tools;

(iii) AI systems intended to be used by or on behalf of law enforcement authorities to evaluate the reliability of evidence in the course of the investigation or prosecution of criminal offences;

(iv) AI systems intended to be used by law enforcement authorities or on their behalf for assessing the risk of a natural person committing or re-committing not solely on the basis of the profiling of natural persons as referred to in regulation 2 of Data Protection (Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties) Regulations, or to assess personality traits and characteristics or past criminal behaviour of natural persons or groups; S.L. 586.08.

(v) AI systems intended to be used by or on behalf of law enforcement authorities for the profiling of natural persons as referred to in regulation 2 of Data Protection (Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties) Regulations in the course of the detection, investigation or prosecution of criminal offences. S.L. 586.08.

(d) high-risk systems used for migration, asylum and border control management, in so far as their use is permitted by law, and these shall include:

(i) AI systems intended to be used by or on behalf of competent public authorities as polygraphs or similar tools;

(ii) AI systems intended to be used by or on behalf of competent public authorities to assess a risk,

including a security risk, a risk of irregular migration, or a health risk, posed by a natural person who intends to enter or who has entered into the territory of Malta;

(iii) AI systems intended to be used by or on behalf of competent public authorities to assist competent public authorities for the examination of applications for asylum, visa or residence permits and for associated complaints with regard to the eligibility of the natural persons applying for a status, including related assessments of the reliability of evidence;

(iv) AI systems intended to be used by or on behalf of competent public authorities in the context of migration, asylum or border control management, for the purpose of detecting, recognising or identifying natural persons, with the exception of the verification of travel documents.

(e) high-risk systems used for administration of justice and democratic processes, and these shall include:

(i) AI systems intended to be used by a judicial authority or on their behalf to assist a judicial authority in researching and interpreting facts and the law and in applying the law to a concrete set of facts, or to be used in a similar way in alternative dispute resolution;

(ii) AI systems intended to be used for influencing the outcome of an election or referendum or the voting behaviour of natural persons in the exercise of their vote in elections or referenda. This does not include AI systems to the output of which natural persons are not directly exposed, such as tools used to organise, optimise or structure political campaigns from an administrative or logistical point of view.

Prohibited AI Practices.

4. The Commissioner shall exercise his tasks and powers in terms of Regulation (EU) 2024/1689 in respect of the following prohibited AI practices:

(a) the placing on the market, the putting into service, or the use of an AI system for making risk assessments of natural persons in order to assess or predict the risk of a natural person committing a criminal offence, based solely on the profiling of a natural person or on assessing his personality traits and characteristics:

Provided that such prohibition shall not apply to AI systems used to support the human assessment of the involvement of a person in a criminal activity, which is already based on objective and verifiable facts directly linked to a criminal activity;

(b) the placing on the market, the putting into service, or the use of AI systems that create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage;

(c) the placing on the market, the putting into service, or the use of biometric categorisation systems that categorise individually natural persons based on their biometric data to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation:

Provided that such prohibition shall not cover any labelling or filtering of lawfully acquired biometric datasets, such as images, based on biometric data or categorising of biometric data in the area of law enforcement;

(d) the use of "real-time" remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement, unless and in so far as such use is strictly necessary for one of the following objectives:

(i) the targeted search for specific victims of abduction, trafficking in human beings or sexual exploitation of human beings, as well as the search for missing persons;

(ii) the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or a genuine and present or genuine and foreseeable threat of a terrorist attack;

(iii) the localisation or identification of a person suspected of having committed a criminal offence, for the purpose of conducting a criminal investigation or prosecution or executing a criminal penalty for offences referred to in Annex II of Regulation (EU) 2024/1689 and punishable by a custodial sentence or a detention order for a maximum period of at least four (4) years.

Designation of fundamental rights authority.

5.[*] The Commissioner, as the supervisory authority responsible for monitoring the applicability of Regulation (EU) 2016/679 and the Act, including all the regulations made thereunder, shall

be designated as the fundamental rights authority for the purpose of Article 77 of Regulation (EU) 2024/1689 insofar as it concerns the right to the protection of personal data:

Provided that the designated role of the Commissioner as a fundamental rights authority shall be without prejudice to the exercise of his tasks and powers as the market surveillance authority as established in regulation 3 and 4.

Use of "real-time" remote biometric identification system in publicly accessible spaces.

6.[*] (1) The use of a "real-time" remote biometric identification system in publicly accessible spaces for the purposes of law enforcement shall only be permissible if its use is strictly necessary for one of the objectives referred to in regulation 4(d).

(2) For the purposes of regulation 4(d) and Article 5(2) of Regulation (EU) 2024/1689, each use of a "real-time" remote biometric identification system in publicly accessible spaces for the purposes of law enforcement shall be subject to a prior authorisation granted by a Magistrate upon a reasoned request:

Provided that in a duly justified situation of urgency, the use of such system may be commenced without an authorisation provided that such authorisation is requested without undue delay, at the latest within twenty-four (24) hours and if such authorisation is rejected, the use shall be terminated with immediate effect and all the data, as well as the results and outputs of that use shall be immediately discarded and deleted.

(3) The Magistrate shall grant the authorisation only where he is satisfied, on the basis of objective evidence or clear indications presented to him, that the use of the "real-time" remote biometric identification system concerned is necessary for and proportionate to, achieving one of the objectives specified in regulation 4(d), as identified in the request and, in particular, remains limited to what is strictly necessary concerning the period of time as well as the geographic and personal scope. In deciding on the request, the Magistrate shall take into account the elements referred to in Article 5(2) of Regulation (EU) 2024/1689. No decision that produces an adverse legal effect on a person may be taken based solely on the output of the "real-time" remote biometric identification system.

(4) Without prejudice to sub-regulation (3), each use of a "real-time" remote biometric identification system in publicly accessible spaces for law enforcement purpose shall also be notified to the Commissioner. The notification shall, as a minimum, contain the

*Not yet in force.
*Not yet in force.

information specified under Article 5(6) of Regulation (EU) 2024/1689 and shall not include sensitive operational data.

(5) Any request to the Magistrate for an authorisation to use "real-time" remote biometric identification systems in publicly accessible spaces shall be made by means of an application, and shall specify in respect of which of the objectives listed in regulation 4(d) is being sought and, where the objective sought is pursuant to regulation 4(d)(iii), the request shall specify for which of the criminal offences referred to in Annex II to Regulation (EU) 2024/1689 the request is being made, and the time-period during which such system shall be in force.

Post-remote biometric identification. S.L. 586.08.

7.[*] (1) Without prejudice to the Data Protection (Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties) Regulations, in the framework of an investigation for the targeted search of a person suspected or convicted of having committed a criminal offence, the deployer of a high-risk AI system for post-remote biometric identification shall request authorisation from the Magistrate by means of an application, *ex ante*, or without undue delay and not later than forty-eight (48) hours, for the use of such system, and subject to the Magistrate providing authorisation for such use, except when it is used for the initial identification of a potential suspect based on objective and verifiable facts directly linked to the offence. Each use shall be limited to what is strictly necessary for the investigation of a specific criminal offence.

(2) If the authorisation requested pursuant to this sub-regulation is rejected, the use of the post-remote biometric identification system linked to such requested authorisation shall be terminated with immediate effect and the personal data linked to the use of the high-risk AI system for which the authorisation was requested shall be deleted.

Notified body for the purpose of high-risk AI systems intended to be put into service by law enforcement, immigration or asylum authorities.

8. For the purposes of the conformity assessment procedure referred to in Annex VII of Regulation (EU) 2024/1689, where the high-risk AI system is intended to be put into service by law enforcement, immigration or asylum authorities, the Commissioner shall act as a notified body.

Documentation.

9.[†] For the purposes of Article 18(2) of Regulation (EU) 2024/1689, a provider or its authorised representative established in Malta which becomes bankrupt or ceases its operation prior to the end

*Not yet in force.
†Not yet in force.

of the period established in Article 18(1) of Regulation (EU) 2024/1689 shall nonetheless keep the documents referred to therein at the disposal of the Commissioner until the period of ten (10) years elapses.

Language requirements.

10.[*] For the purpose of Article 23(6) of Regulation (EU) 2024/1689, importers shall provide the Commissioner upon a reasoned request, with all the necessary information and documentation, including that referred to in Article 23(5) of Regulation (EU) 2024/1689, to demonstrate the conformity of a high-risk AI system with the requirements stipulated in Section 2 of Regulation (EU) 2024/1689 in either the Maltese or English Language.

High-risk AI systems register.

11.[†] The Commissioner shall establish a registry for the national registration of high-risk AI systems listed in regulation 3.

Right to submit a complaint.

12.[‡] (1) Without prejudice to other administrative or judicial remedies, any natural or legal person having grounds to consider that there has been an infringement of the provisions of these regulations or of Regulation (EU) 2024/1689 may submit a complaint to the Commissioner as the designated market surveillance authority pursuant to these regulations. In accordance with Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011, such complaints shall be taken into account for the purpose of conducting market surveillance activities, and shall be treated in accordance with the dedicated procedures established therefor by the market surveillance authorities.

(2) Sub-regulation (1) shall be without prejudice to the right of a data subject under Regulation (EU) 2016/679 to submit a complaint with the Commissioner as fundamental rights authority if the data subject considers that the processing of personal data relating to him infringes Regulation (EU) 2016/679. In this case the provisions of Chapters VI, VII and VIII of Regulation (EU) 2016/679 shall apply *mutatis mutandis.*

Administrative penalties.

13. (1) The Commissioner, as the designated market surveillance authority pursuant to these regulations, may institute enforcement action applicable to infringements of the Regulation (EU) 2024/1689 and these regulations committed by operators. This may include the imposition of administrative penalties, warnings and non-monetary measures:

*Not yet in force.
†Not yet in force.
‡Not yet in force.

Provided that article 20 of the Act shall *mutatis mutandis* apply to any decision issued by the Commissioner in the enforcement of the provisions of Regulation (EU) 2024/1689 and these regulations. An appeal shall lie to the Information and Data Protection Appeals Tribunal from any decision taken by the Commissioner and Part VI of the Act shall apply *mutatis mutandis*.

(2) When deciding whether to impose an administrative penalty and in determining the amount of the administrative penalty in each individual case, all relevant circumstances of the specific situation shall be taken into account and, as appropriate, regard shall be given to the following:

(a) the nature, gravity and duration of the infringement and of its consequences, taking into account the purpose of the AI system, as well as, where appropriate, the number of affected persons and the level of damage suffered by them;

(b) whether administrative penalties have already been applied by other market surveillance authorities to the same operator for the same infringement;

(c) whether administrative penalties have already been applied by other authorities to the same operator for infringements of other Union or national law, when such infringements result from the same activity or omission constituting a relevant infringement of these regulations and of Regulation (EU) 2024/1689;

(d) the size, the annual turnover and market share of the operator committing the infringement;

(e) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement;

(f) the degree of cooperation with the Commissioner, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

(g) the degree of responsibility of the operator taking into account the technical and organisational measures implemented by him;

(h) the manner in which the infringement became known to the Commissioner, in particular whether, and in that case to what extent, the operator notified the infringement;

(i) the intentional or negligent character of the infringement;

(j) any action taken by the operator to mitigate the harm suffered by the affected persons.

(3) The Commissioner, as the case may be, after giving due regard to the circumstances of the case shall impose an administrative penalty on a public authority or body:

Provided that such an administrative penalty shall not exceed fifty thousand euro (€50,000) for each infringement and additionally, the Commissioner, as the case may be, may impose a daily penalty of fifty euro (€50) for each day during which such infringement persists.

(4) At any stage of the proceedings in relation to an infringement of these regulations and of Regulation (EU) 2024/1689, the Commissioner may require any person, or public authority or body, which has infringed any provision of these regulations or of Regulation (EU) 2024/1689 to undertake in writing to refrain from such conduct and to take any remedial or other action as the Commissioner, may specify.

(5) The initiation of proceedings by the Commissioner shall be prescribed by the lapse of two (2) years from the date on which the infringement is alleged to have been committed.