

Annual Report
& Financial Statements

20
25



Contents

01	Key Performance Figures	3
02	Foreword	6
03	Mission, Vision & Strategic Objectives	10
04	Organisation	12
4.1	Organigram and Staff Complement	
4.2	Financial Resources	
05	Our Initiatives and Engagements	15
5.1	Participation in the EDPB Coordinated Enforcement Framework	
5.2	EU and International Engagements	
5.3	Fundamental Rights Impact Assessment (FRIA) Workshop	
5.4	European Blockchain Sandbox (third cohort)	
5.5	Local engagements	
5.6	Engagement with Local Regulatory Authorities	
5.7	DISC Research Cluster	
5.8	Recognition of Research Ethics Committee – Mater Dei Hospital	
5.9	Delivery of data protection lectures – Employment course – MEA	
5.10	Proactive Engagement with Healthcare Providers on Data Protection Officer Requirements	
5.11	Contributions to Privacy Laws and Business and MLex	
5.12	Publication of FAQs	
06	Data Protection Regulatory Work	34
6.1	Contacts and Enquiries	
6.2	Advisory Services	
6.3	Complaints	
6.4	Ex-Officio Investigations	
6.5	One-Stop-Shop Cases	
6.6	Personal Data Breaches	
6.7	Administrative Fine imposed by the Commissioner	
6.8	Supervisory Audits	
07	Freedom of Information	58
08	Financial Statements	62
	Commissioner's Report	
	Independent Auditor's Report	
	Statements of Profit or Loss and Other Comprehensive Income	
	Statement of Financial Position	
	Statement of Changes in Equity	
	Statement of Cash Flows	
	Notes to the Financial Statements	

01

Key Performance Figures

01

Key Performance Figures

Complaints

701
Total Complaints Received

182
Admissable Complaints

147
Rejected Complaints

122
Dismissed Complaints

75%
of admissible cases
led to a finding of
infringement

One-Stop-Shop Cases

535
Total One-Stop-Shop
cases

517
Lead Supervisory
Authority (LSA) cases

450
Related to right of
access requests

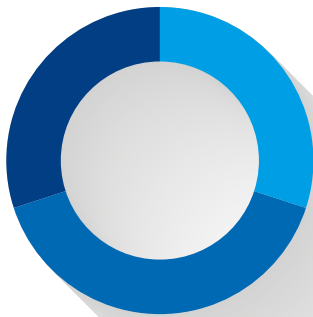
8
Concerned Supervisory
Authority (CSA) cases

01

Key Performance Figures

Freedom of Information Applications

Decision notices issued:



Justified: 3
Not justified: 4
Partially justified: 3

667

Total Number of Requests received by Public Authorities

52

FOI Applications handled by IDPC

12

Resolved through amicable settlement between the parties

Data Breaches

114

Total breaches reported

23

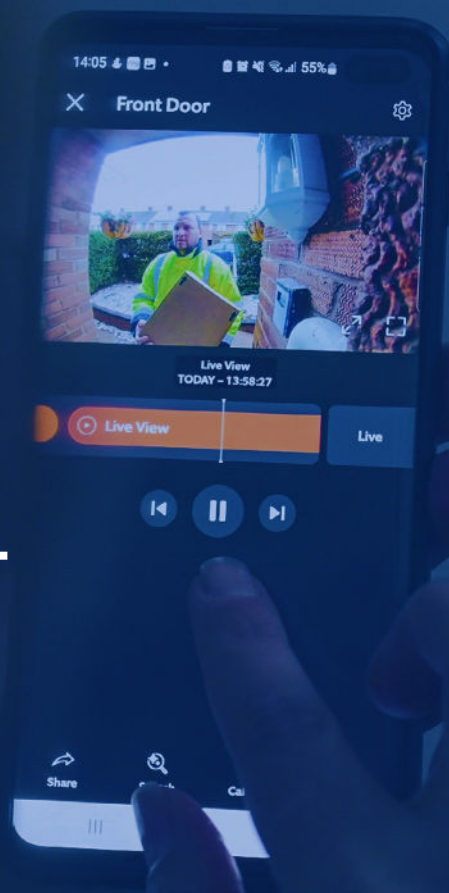
Financial Sector most affected by these breaches

45

Cyber-attacks including phishing and ransomware

02

Foreword



I am pleased to present the Annual Report of the Office of the Information and Data Protection Commissioner covering the year 2025 – a year that continued to highlight the central role of data protection in an increasingly complex and rapidly evolving digital landscape.



At the outset, I would like to acknowledge the work carried out by my predecessor, Mr Ian Deguara, under whose leadership the office continued to strengthen its supervisory and regulatory functions. The achievements presented in this report reflect a sustained commitment to upholding the fundamental rights of individuals while ensuring that organisations process personal data in a lawful and responsible manner. I am honoured to build on this solid foundation following my appointment as Commissioner with effect from 24 April 2026.

During 2025, the office experienced a continued increase in activity across its core functions. This was particularly evident in the rise of complaints and queries received from both individuals and organisations. Individuals are becoming more aware of their rights under data protection law and are increasingly confident in exercising them. At the same time, data controllers and processors are seeking more guidance on their obligations, reflecting a growing recognition that compliance must be embedded into organisational practices.

A notable feature of the year under review was the continued prominence of cross-border cases. As more organisations operate in multiple jurisdictions, cooperation with other supervisory authorities within the European Union remains essential. The effective functioning of the one-stop-shop mechanism continues to play a key role in ensuring consistency and efficiency in the handling of such cases. Our office has remained actively engaged in these processes, contributing to joint efforts aimed at safeguarding data subjects' rights across borders.

The ongoing digital transformation across both the public and private sectors has also brought new challenges to the fore. The increasing reliance on data-driven technologies has heightened the need for robust data governance frameworks. In particular, the use of artificial intelligence has continued to raise important questions regarding transparency, fairness, and accountability. While these technologies offer significant opportunities for innovation and economic development, they must be deployed in a manner that fully respects fundamental rights.

“ A notable feature of the year under review was the continued prominence of cross-border cases. ”

In this context, and as reflected in developments during 2025, the office has assumed an increasingly important role within the evolving European regulatory framework governing artificial intelligence.



Following the entry into force of the Artificial Intelligence Act, the IDPC has been designated as the Fundamental Rights Authority insofar as the protection of personal data is concerned.

Following the entry into force of the Artificial Intelligence Act, the IDPC has been designated as the Fundamental Rights Authority insofar as the protection of personal data is concerned. In addition, the office is expected to be designated as a Market Surveillance Authority responsible for overseeing certain high-risk AI systems, particularly in areas such as law enforcement, border management, and the administration of justice. These functions place the office at the forefront of ensuring that AI systems affecting individuals are deployed in a manner that safeguards their rights, including the right to privacy and data protection, while also promoting transparency, robustness, and accountability in their operation.

Another important aspect of the office's work during the year relates to its advisory function. The Commissioner has been consulted on a number of legislative initiatives involving the processing of personal data. This process ensures that data protection considerations are integrated at an early stage in the development of legal instruments. Such engagement contributes to the creation of legislation that is both effective and aligned with the requirements of the General Data Protection Regulation (GDPR).

The report also highlights the office's continued efforts in raising awareness and providing guidance.

Outreach initiatives, engagement with stakeholders, and the publication of guidance materials have all contributed to promoting a better understanding of data protection obligations. These efforts are essential in fostering a culture of compliance and accountability across all sectors.

In line with this approach, the office organised a dedicated workshop in October 2025 focusing on Fundamental Rights Impact Assessments (FRIA) under the Artificial Intelligence Act. This initiative brought together national and international expertise and addressed the practical application of FRIA methodologies, particularly in the context of high-risk AI systems. The workshop also examined the complementarity between the GDPR and the AI Act, highlighting the synergies between FRIA and Data Protection Impact Assessments (DPIAs), and how these processes can be aligned to enhance the protection of individuals' rights.

The interactive and practice-oriented nature of this workshop, including the use of case studies and expert-led discussions, provided participants with valuable insight into identifying and assessing risks to fundamental rights in AI deployments. Initiatives of this nature will continue to form an integral part of the office's work, as we seek to equip stakeholders with the tools and knowledge necessary to navigate an increasingly complex regulatory environment, while ensuring that innovation remains firmly anchored in respect for fundamental rights.

It is also worth noting that the office has maintained its focus on enforcement where necessary. While guidance and support remain key priorities, effective supervision requires that appropriate action is taken in cases of non-compliance. Enforcement measures are essential not only to address individual infringements but also to reinforce public trust in the regulatory framework.

At the European level, developments during 2025 have continued to shape the broader landscape within which data protection operates. Ongoing discussions and initiatives aimed at enhancing cooperation and streamlining procedures, particularly in relation to cross-border enforcement, will have

Despite our small staff complement, a significant amount of work has been accomplished. Like our European counterparts, we are experiencing a steady increase in the number of complaints received, which is placing additional pressure on our available resources. In the age of artificial intelligence and rapid digitalisation, this growing caseload will inevitably require the allocation of further resources, which we are confident can be secured as needed.

In this regard, I would like to express my appreciation for the continued cooperation and support provided by the Ministry of Justice. The Ministry has consistently demonstrated its readiness to assist, enabling us to fulfil our statutory obligations effectively and to deliver an efficient and high-quality service to our stakeholders.

Finally, I wish to place on record my sincere appreciation for the professionalism, dedication, and commitment of our staff. Their unwavering efforts, often extending beyond the requirements of their respective roles, have been instrumental in ensuring the effective discharge of the Office's responsibilities and in providing assistance to all those who seek our services.

The achievements outlined in this Report are a testament to their hard work and expertise throughout 2025. Their contribution has been central to advancing the Office's mandate and objectives, and their continued commitment will remain vital to meeting future challenges and delivering high standards of service to our stakeholders.

Dr Reno Borg
Information and Data Protection
Commissioner
Malta

“ Looking ahead, the challenges associated with emerging technologies, increasing data flows, and evolving regulatory frameworks will require a proactive and forward-looking approach. ”

an important impact on the work of supervisory authorities. The office remains committed to contributing constructively to these processes.

Looking ahead, the challenges associated with emerging technologies, increasing data flows, and evolving regulatory frameworks will require a proactive and forward-looking approach. The office will continue to adapt its practices and strengthen its capabilities to respond effectively to these developments. At the same time, our guiding principle remains unchanged: to protect the rights and freedoms of individuals while enabling responsible and lawful data processing.

We remain steadfast in our commitment to a rights-based approach – one that ensures that innovation is accompanied by strong safeguards, and that individuals retain control over their personal data. Supporting organisations in meeting their obligations, while placing individuals at the centre of our work, will remain a core priority.

03

Mission, Vision and Strategic Objectives



Our mission is to ensure that the individuals' fundamental right to the protection of their personal data is safeguarded and guaranteed, as well as, to facilitate the right to access to information held by public authorities in pursuit of promoting added transparency and accountability in the public administration.

Our vision is to foster an open society in which individuals have full confidence that their right to the protection of personal data is effectively safeguarded, while simultaneously enjoying the right to freedom of information. Through the realisation and protection of these fundamental rights, we seek to reinforce individual liberties and contribute to the advancement of a robust and inclusive democratic society.

During 2025, the Commissioner's key strategic objectives to achieve his mission and vision in a digital ecosystem shaped by new and emerging technologies, were:

- » to promote compliance with the data protection legal framework by emphasising the accountability principle among data controllers and processors, while encouraging the implementation of data protection by design for new systems;
- » to safeguard individuals' data protection rights by investigating and resolving complaints in a timely and fair manner;
- » to closely follow the developments at European level relating to the changes proposed by the European Commission, by virtue of the Digital Omnibus, to the data protection legal framework;
- » to promote awareness and education by raising awareness on data protection principles and rights to the general public and engage with associations and constituted bodies to provide tailored advice;
- » to actively support the government when requesting data protection advice on new legislation which involves the processing of personal data;
- » to build the appropriate internal human resources and competences, mainly through upskilling, to be in a position to effectively fulfil its regulatory role and appropriately address any challenges brought about by new and emerging technologies.

“ Through the realisation and protection of these fundamental rights, we seek to reinforce individual liberties and contribute to the advancement of a robust and inclusive democratic society. ”

04

Organisation

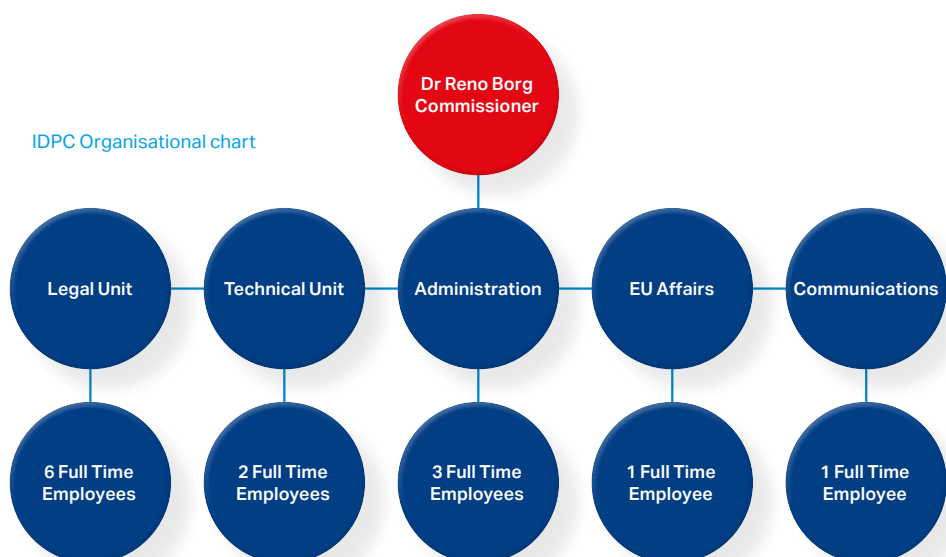


04

Organisation

4.1

Organigram and Staff Complement



As of 24 April 2026

During the year under review, the office strengthened its organisational structure through the establishment of two key functions: one dedicated to communications and another focused on international and European affairs. To support these new functions, two senior officers were recruited.

The communications function was established to enhance the visibility of the office's regulatory work and to develop effective outreach strategies aimed at increasing

awareness and understanding of data protection rights and obligations, particularly among data subjects.

The international and European affairs function will enable the office to engage more actively and effectively in the work of the European Data Protection Board (EDPB), as well as in other international forums and commitments. This enhanced capacity will ensure that the office remains well-positioned to contribute to, and benefit from, developments in the European and international data protection landscape.

4.2

Financial Resources

The financial resources allocated to the office during 2025, as a budget line within the Ministry for Justice, amounted to €800,000. This represents an increase of €50,000 over the allocation provided in the previous year.

The Commissioner remains confident that the Government fully recognises the important role of the office,

particularly in view of the expanding responsibilities with which it has been, and will continue to be, entrusted. These additional functions require the office to maintain the necessary resources and capacity to effectively fulfil its regulatory, supervisory, and enforcement responsibilities.

4.3

Legislative Developments

The IDPC was responsible for drafting and publishing the following legal notices:

- » Legal Notice 227 of 2025, the **Artificial Intelligence** (Designation of the Information and Data Protection Commissioner for the Purposes of Regulation (EU) 2024/1689) **Regulations** – subsidiary legislation 586.14 under the Data Protection Act; and
- » Legal Notice 223 of 2025, the Data Protection (**Fair Access to and Use of Data**) **Regulations** – subsidiary legislation 586.13 under the Data Protection Act.

The AI regulations under the Data Protection Act

Legal Notice 227 of 2025 (the 'AI Regulations') transposes the EU AI Act (Regulation (EU) 2024/1689) into Maltese law, while introducing targeted adaptations to augment the framework with the national legal framework. It designates the IDPC as the Market Surveillance Authority responsible for overseeing specific high-risk AI systems, particularly in areas such as law enforcement, border control, emergency services, and the administration of justice.

The notice also incorporates domestic-specific procedural safeguards, including the requirement of prior authorisation by a Magistrate for the use of real-time and post-remote biometric identification systems in publicly accessible spaces, as well as notification obligations to the Commissioner.

In addition, it grants the IDPC enforcement powers in line with the EU framework and the Data Protection Act where an infringement of the EU AI Act or the AI Regulations is suspected, including the ability to investigate infringements and impose administrative penalties, warnings, and corrective measures, with capped fines applicable to public authorities under Maltese law.

Data Act regulations under the Data Protection Act

Legal notice 223 of 2025 (the 'Data Act regulations') transposes the EU Data Act (Regulation (EU) 2023/2854) into Maltese law.

The EU Data Act is aimed at unlocking the potential of the industrial and consumer data economy, being typically comprised of data generated by devices connected to the Internet of things (IoT-connected devices), by promoting fair data sharing of such data whilst ensuring the protection of personal data which may be a part of IoT data.

The Data Act regulations designate the IDPC as the competent authority responsible for monitoring, the application of the EU Data Act where the protection of personal data is concerned, whilst making it clear that concerned individuals may lodge a complaint with the Commissioner where processing activities carried out, in terms of such Data Act regulations is suspected to infringe the provisions of the EU GDPR.

05

Our Initiatives and Engagements



5.1

Participation in the EDPB Coordinated Enforcement Framework (CEF)

The Coordinated Enforcement Framework (CEF) was developed by the EDPB to streamline enforcement and strengthen cooperation among supervisory authorities (SAs) and is a key action of the same EDPB under its 2024-2027 Strategy. It creates a structure for SAs to work together, coordinate and/or facilitate enforcement actions on a pre-defined topic using an agreed-upon methodology. The legal basis for the CEF is found in Article 57(1) (g) of the GDPR, which gives national SAs the competence to *“cooperate with, including sharing information and provide mutual assistance to, other supervisory authorities with a view to ensuring the consistency of application and enforcement of this Regulation.”*

Each year, SAs select the priority enforcement topic on which they will act in a coordinated way. In 2025, the chosen topic for the fourth coordinated enforcement action was the 'Implementation of the Right to Erasure (Right to be Forgotten) by Controllers' in terms of Article 17 of the GDPR. The main reason behind the selection of this topic by the EDPB was the fact that it is considered as one of the most frequently exercised data GDPR rights and ultimately one about which SAs frequently receive

queries or complaints from affected data subjects. SAs including the IDPC used this exercise to analyse how data controllers handle and respond to requests for erasure they receive and how they apply the conditions and exceptions for the exercise of this right.

The overall assessment which emerged during the local investigation carried out by the IDPC is encouraging particularly due to some best practices observed. The full CEF report as published by the EDPB indicates a number of main implementation problems or challenges that were observed in respect of some controllers thus hindering the full implementation of the right to erasure. However, a number of best practices have also been identified by the EDPB. In this context this report is presented with a series of recommendations to effectively implement the right to erasure. The overall level of compliance was identified by the EDPB as “average”.

More information on the CEF may be accessed on the following link:

https://www.edpb.europa.eu/coordinated-enforcement-framework_en

5.2

EU and International Engagements

Throughout 2025, the IDPC continued to actively engage with European and international counterparts, with a view to strengthening cooperation, promoting consistency in enforcement practices, and ensuring alignment with evolving global developments in the field of data protection.



Data Protection Conference in Moldova – January 2025

The Commissioner took part in a conference on "New Legal Provisions in Personal Data Protection in Moldova", held on Data Protection Day in Moldova's capital Chisinau. The conference was organised by e-Governance Academy in partnership with the National Centre for Personal Data Protection of the Republic of Moldova.

During his intervention, Commissioner Deguara explained the complementary roles of data protection and

cybersecurity, stressing the broader impact of failures on both reputation and fundamental rights.

The conference featured a number of speakers and covered several topics such as aligning Moldova's data protection regulations with EU standards; challenges posed by emerging technologies like AI; rights, responsibilities, and breach management in data processing as well as strengthening privacy protection through cybersecurity.

05

Our Initiatives and Engagements

5.2

EU and International Engagements



British, Irish and Islands Data Protection Authorities (BIIDPA) Meeting, Guernsey – 25 to 26 June 2025

BIIDPA is a network that links the data protection authorities of Malta, Bermuda, Cayman Islands, Cyprus, Gibraltar, Guernsey, Ireland, Isle of Man, Jersey and the United Kingdom, thus bringing together ten data protection authorities from two continents. These authorities, though having their own separate data protection regimes, have close affinities, and thus, strive to ensure practical supervisory consistency through this network.

The IDPC was among the supervisory authorities that took part in the BIIDPA 2025 annual meeting, which was held in Guernsey between 25 and 26 June 2025. Hosted by the Bailiwick of Guernsey's Office of the Data Protection Authority, the meeting provided a forum

for discussing shared enforcement challenges, exchanging case-handling experiences, and exploring ways to promote data protection rights while enabling responsible innovation across their jurisdictions.

Among the key topics of discussion were the promotion and protection of children's privacy rights, the importance of having strong data protection practices as a foundation for sustainable technological innovation, the role of international cooperation in improving the overall protection of data protection rights, and the need for supervisory authorities to adopt modern, practical and proportionate approaches to data protection enforcement.

05

Our Initiatives and Engagements

5.2

EU and International Engagements



Global Privacy Assembly (GPA) – 15 to 19 September 2025

The office participated in the 47th Global Privacy Assembly (GPA), held in Seoul, South Korea between 15 and 19 September 2025. The event was hosted by the Personal Information Protection Commission of Korea and centred on the theme "Artificial Intelligence in Our Daily Lives: Data and Privacy Issues".

The Assembly addressed a wide range of topics reflecting current global challenges in data protection. These included data governance in the context of artificial intelligence, the use of pseudonymisation to support innovation, lawful bases for processing data for AI-related purposes and the need to reassess

data protection frameworks in light of emerging technologies. Discussions also covered cross-border data transfers, interoperability between legal frameworks and the protection of children's privacy in the context of educational technologies.

The GPA is a leading international forum that brings together data protection and privacy authorities from across the world. Established in 1979 as the International Conference of Data Protection and Privacy Commissioners, it has since evolved into a global platform comprising more than 140 authorities from over 90 countries.

05

Our Initiatives and Engagements

5.2

EU and International Engagements

The assembly plays a key role in fostering international cooperation and promoting high standards of data protection. It provides a forum for supervisory authorities to exchange knowledge, share national experiences, and contribute to the development of global privacy standards. Through its resolutions and declarations, the GPA encourages consistent and robust approaches to data protection across jurisdictions.

Participation in the assembly enables the office to remain informed of international developments, contribute to ongoing policy discussions, and strengthen collaboration with other supervisory authorities, as well as stakeholders from academia, industry and international organisations.



Signing of MOU with Information Commissioner of the Isle of Man

On the sidelines of the GPA, the office and the Information Commissioner of the Isle of Man signed a Memorandum of Understanding (MoU) to strengthen their existing relations and to promote exchanges to assist each other in the delivery of their regulatory functions.

The MoU provides a framework for the Commissioners to cooperate in a way that supports their data-driven economies while protecting the

fundamental rights of citizens in Malta and the Isle of Man, in accordance with their applicable data protection laws. It also establishes mechanisms for regular communication on matters of mutual interest, share knowledge and consult each other on issues that have a significant implication on both offices, while cooperating with respect to the enforcement of their respective applicable data protection laws.

5.2

EU and International Engagements

EDPB bootcamp – 1 to 2 October 2025

Technical and legal officers from this office participated in the third EDPB bootcamp held in Brussels at the organisation's premises. Held on 1 and 2 October 2025, its aim was to enhance both legal and technical expertise within supervisory authorities.

The first day of the bootcamp involved the continuance on prior work on mobile applications, featuring a hands-on SDK analysis workshop supported by PEReN, using Pirogue datasets. The programme also focused on artificial intelligence, combining practical exercises such as algorithm development with presentations on AI, the AI Act, and data protection.

The second day of the bootcamp addressed key challenges in AI supervision, including emerging attack techniques, auditing of AI systems, and supervisory experiences with machine learning. It also addressed ongoing Support Pool of Experts (SPE) projects on topics such as algorithmic bias, unlearning, and privacy risks in AI technologies.

The bootcamp concluded with discussion on ensuring future collaboration in AI auditing. The IDPC's participation strengthened its capacity to address the data protection implications of emerging technologies, especially where AI or other data training models may be involved.

**European Case Handling Workshop (ECHW), Prishtina, Kosovo – 17 to 19 November 2025**

This office participated in the European Case Handling Workshop (ECHW), which was hosted for the first time by the Information and Privacy Agency in Prishtina, Kosovo, between 17 and 19 of November 2025.

The ECHW brought together around 70 representatives from data protection authorities across

23 European countries, including Albania, Austria, Belgium, Croatia, Czechia, Estonia, Germany, Guernsey, Hungary, Ireland, Luxembourg, Malta, the Netherlands, North Macedonia, Norway, Poland, Sweden, Switzerland, Turkey, and the United Kingdom.

5.2

EU and International Engagements

European Case Handling Workshop (ECHW), Prishtina, Kosovo – 17 to 19 November 2025

During the ECHW, data protection experts and decision-makers addressed key issues shaping the development of data protection standards. The discussions focused on the use of smart cameras and biometric data in public spaces, the phenomenon of deepfakes and AI-generated content, the protection of children's data on digital platforms, challenges related to data scraping and the use of publicly accessible data, as well as cross-border cooperation and the processing of health data in the era of digitalisation.

The workshop provided a valuable opportunity for representatives of European data protection authorities to exchange experiences on investigating complaints, issuing guidance to controllers, and enforcing data protection law. It also enabled representatives to engage in productive discussions and gain valuable insights into how other data protection authorities are addressing

emerging data protection challenges and promoting public awareness of data protection within their territories.

Council of Europe – T-PD

Malta, being a party to the 'Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data' (Convention ETS no. 108), is a member of the consultative committee (T-PD) set up in terms of Chapter V of this Convention, which meets regularly in November and June, and is entrusted inter alia to make proposals to facilitate or improve the application of the Convention and to suggest amendments to the same Convention.

As in previous years, this office made its contribution to this international forum by participating in its plenary meetings which focused on the evaluation and follow-up mechanism under Convention 108+, children's data protection in an education setting, facial recognition and profiling and the transborder data flows of personal data among others.

5.3

Fundamental Rights Impact Assessment (FRIA) Workshop



The office successfully organised a full-day workshop on 23 October 2025 focused on the requirement to conduct a Fundamental Rights Impact Assessment (FRIA) under Article 27 of the AI Act.

The workshop was held in close collaboration with Professor Alessandro Mantelero, an acclaimed Associate Professor of Private Law and Law & Technology at the Polytechnic University of Turin. During the event, Prof. Mantelero shared his extensive experience on the importance of carrying out a fundamental rights impact assessment – even in cases where it is not legally required – prior to deploying or implementing a high-risk AI system. He also provided participants with valuable insights into the background of the project, explaining how it came to fruition and the rationale for basing the FRIA model on matrices rather than numerical values.

The workshop further explored the complementarity between the GDPR and the AI Act, highlighting the synergies between the FRIA and the Data Protection Impact Assessment

(DPIA). Participants examined how these two assessment processes can be aligned to streamline compliance efforts and strengthen the protection of individuals' rights, particularly in high-risk AI applications involving personal data processing.



5.3

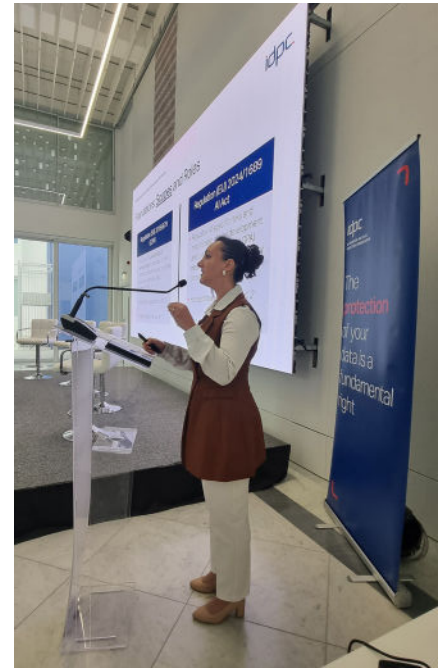
Fundamental Rights Impact Assessment (FRIA) Workshop

The event featured a keynote address delivered by Commissioner Ian Deguara, as well as a presentation on the interplay between the AI Act and the GDPR by Dr Penelope Micallef Vassallo, Legal and European Affairs Senior Officer at the IDPC.

A panel discussion was held with the theme being “Navigating the Risks and Challenges to Fundamental Rights in the era of AI” and was moderated by former Commissioner Deguara.

During the second half of the day, participants were divided into groups and presented with a practical use-case on which they applied the methodology introduced during the morning session. Each group was tasked with identifying the fundamental rights potentially affected and subsequently assessing the likelihood and severity of the risks to those rights. The groups then presented their findings, which were reviewed and discussed by Prof. Mantelero, providing valuable insights into the practical application of the FRIA model.

The discussions and feedback gathered throughout the workshop offered meaningful contributions to the IDPC’s ongoing efforts to promote the importance of risk assessments. They also served as a valuable resource in supporting organisations as they prepare to meet the evolving obligations set out under the AI Act, while ensuring the protection of individuals’ fundamental rights remains at the core of AI deployment.



5.4

European Blockchain Sandbox (third cohort)

The office has previously participated in the first and second cohorts of the European Blockchain Sandbox (EBS), a voluntary EU-level initiative facilitating regulatory dialogue on innovative blockchain use cases. In 2025, the office participated once again as one of the selected EU/EEA authorities in the third cohort, which combined blockchain with AI and IoT proposed solutions.

The third cohort brought together a broad range of regulators and authorities across Europe, including data protection authorities, financial regulators, central banks, and EU institutions. Selection followed a competitive process overseen by independent academic experts, reflecting the high level of participation and interest in emerging technologies.

The IDPC joined structured regulatory dialogues coordinated by the EBS team (led by Bird & Bird and OXYGY), which aim to explore legal and regulatory issues arising from real-world blockchain applications. These dialogues were scheduled to take place between June and November 2025.

The initiative will conclude with the publication of a best practices report, capturing regulatory insights from participating authorities.

Through this engagement, the IDPC contributed to EU-level cooperation and knowledge-sharing on emerging technologies, supporting consistent interpretation of data protection requirements in innovative blockchain contexts.

5.5

Local engagements

AI and Data Protection

The office undertook an extensive programme of outreach and awareness raising with the public and stakeholders in 2025, focusing on the intersection of data protection and artificial intelligence (AI), particularly in light of the EU AI Act.

At national level, the IDPC and officials actively contributed to high-level events, including a Data Protection Day, organised by the Ministry of Justice. This included presentations on enforcement activity and casework, as well as expert-led sessions addressing emerging AI-related data protection challenges, demonstrating the IDPC's dual role in both supervision and public education.

A significant part of its work involved sector-specific engagement, providing targeted guidance across key areas:

- » **Education sector:** Seminars, panels, and keynote interventions (including with MDIA and MCAST) addressed AI in admissions, grading, and assessment, stressing high-risk use, Article 22 GDPR compliance, and the need for human oversight, fairness, and DPIAs/FRIAs.
- » **Employment and recruitment:** Discussions focused on AI hiring and monitoring tools, highlighting their intrusive nature, high-risk classification, limits on processing in employment, consent concerns, and safeguards against discrimination.

05

Our Initiatives and Engagements

5.5

Local engagements



- » **Gaming sector:** Engagement addressed risks from AI-driven profiling and manipulation, including prohibited AI practices under the AI Act and the need to protect vulnerable users.
- » **Business and cross-sector stakeholders:** Panels focused on compliance, stressing data protection by design and by default and clarifying DPIA–FRIA relationships, supported by capacity-building initiatives.
- » **Technical community:** A seminar examined GDPR and AI Act application to AI systems, including analysis of large language models and their data processing lifecycle.
- » **Professional and regulatory bodies:** Guidance focused on balancing transparency obligations with GDPR principles such as necessity, proportionality, and data minimisation.

Across all activities, the office emphasised the high-risk nature of AI systems, human oversight, risks of automated decision-making, and embedding fundamental rights compliance at the design stage.



In parallel, the IDPC strengthened its institutional role through collaboration with the Malta Digital Innovation Authority (MDIA), EU-level engagement, and consolidation of its role as both a data protection and fundamental rights authority.

The office was invited by ISACA Malta Chapter to deliver an educational talk with the topic selected being ‘*Navigating Security Incidents that lead to Personal Data Breaches from a GDPR perspective*’.

Overall, these initiatives demonstrate a proactive approach, combining regulatory oversight with sustained stakeholder engagement to support responsible AI deployment in Malta.

05

Our Initiatives and Engagements

5.5

Local engagements



Podcasts

The IDPC further complemented its outreach through a dedicated podcast series, providing an accessible platform to raise awareness on data protection and AI-related issues.

Episodes featured the Commissioner and senior officials offering insights into the IDPC's role, enforcement work and the protection of personal data as a fundamental right under the GDPR, amongst other topics. A key focus was the impact of artificial intelligence on fundamental rights, including the importance of transparency, accountability, and tools such as Fundamental Rights Impact Assessments (FRIAs) to support human-centric AI.

The series also delivered practical guidance on GDPR obligations, covering data subject rights, common complaints, data processing principles, and the compliant use of technologies such as CCTV. In parallel, it addressed EU-level regulatory developments, including proposed GDPR reforms, and their implications for data protection.

Overall, the podcast series highlights the IDPC's commitment to public engagement, regulatory guidance, and awareness-raising on evolving data protection challenges.

Issuing of IDPC Newsletter

In 2025, the office started issuing regular informative newsletters on various topics relating to the IDPC as well as the latest local and international news related to data protection, GDPR, AI and many other topics. Those wanting to receive the newsletter in their inbox can do so by registering on the IDPC website via this [link](#). Likewise, social media users are encouraged to stay up to date by following the IDPC LinkedIn page via this [link](#).

Participation in radio programme on Radio Malta

As part of its ongoing outreach efforts, the office regularly took part in a live radio programme featuring listener call-ins, during which a range of data protection topics were discussed. These discussions were specifically tailored to the programme's audience, which largely comprises individuals who are not data protection specialists but are nevertheless aware of their rights and willing to share concerns relating to matters affecting their everyday lives. The Commissioner gave due consideration to such concerns, and on select occasions, callers were invited to submit detailed information to the office to enable the initiation of ex officio investigations where appropriate.

5.6

Engagement with Local Regulatory Authorities

The office actively participated in a series of Fundamental Rights Authorities' Roundtable meetings, coordinated by the MDIA, bringing together key national bodies responsible for the protection of fundamental rights.

These roundtables established a structured platform for cross-sectoral dialogue and cooperation in the context of the EU AI Act, particularly in line with Article 77, which recognises the role of fundamental rights authorities in the AI governance framework. The IDPC contributed its expertise as the authority responsible for data protection, ensuring that the right to the protection of personal data and privacy remained central to discussions.

Engagements focused on the roles and responsibilities of authorities under the AI Act, anticipated legislative developments, and the adoption of Terms of Reference to support sustained inter-institutional cooperation. Discussions also emphasised the need for AI systems to remain human-centric, lawful, and non-discriminatory, particularly in relation to vulnerable individuals.

Through its participation, the IDPC reinforced coordinated national approaches to AI governance, ensuring

that data protection is effectively integrated within the broader fundamental rights framework.

The IDPC also maintained engagement with the Malta Communications Authority (MCA), and other concerned entities, in the context of the implementation of the EU Digital Services Act (DSA), supporting national coordination efforts and alignment with EU regulatory requirements.

This engagement focused on ensuring that data protection considerations are appropriately integrated into DSA implementation, particularly in relation to safeguards for minors, including restrictions on targeted advertising based on profiling on online platforms, and the prohibition of processing special categories of personal data on online platforms for the purposes of profiling.

This is a reflection of the IDPC's commitment to support inter-institutional cooperation with authorities such as the MCA to ensure at national level the appropriate application of technology-based frameworks such as the DSA which will, inevitably, intersect with other prominent data focussed frameworks, particularly the GDPR.

5.7

DISC Research Cluster

In 2025, the Commissioner was invited by researchers from an educational institution to establish and participate in a forum to discuss the persistent challenges encountered when conducting scientific research involving special categories of personal data. The forum was established primarily to explore how these challenges could be addressed in the most effective and coordinated manner, whilst safeguarding the right to the protection of personal data.

Following extensive discussions in 2025, including consultations with other relevant stakeholders, the forum presented legislative amendments to the Government for consideration. These proposed regulations draw on comparative laws from other Member States and aim to address the current piecemeal approach in the legislation by establishing a more coherent and comprehensive legislative framework. The objectives of the proposed regulations, which are intended to be introduced under the Data Protection Act, Chapter 586 of the Laws of Malta, are as follows:

» **Enable a lawful basis for the processing of a special category of personal data for scientific research purposes.** The proposed regulations will provide a derogation from the prohibition in article 9(1) of the GDPR for scientific research projects that meet the requirements of proportionality, data minimisation, and other appropriate measures specified in the regulations. This will provide legal certainty to controllers and processors and encourage responsible scientific research.

- » **Institute independent ethics oversight.** A Commissioner-designated ethics committee, with mandatory data-protection expertise, will be established to pre-approve each research project. The committee will have the power to revoke approvals in case of non-compliance and will be subject to audits by the Commissioner, thereby embedding accountability in the research process.
- » **Establish a licensing regime for registered data banks.** Any Maltese entity that curates research datasets will be required to obtain a renewable ten-year permit, comply with defined security standards, maintain detailed access logs, and be listed in a publicly accessible register.
- » **Lay down uniform safeguards for research processing in the context of data banks.** Controllers responsible for processing data within data banks must conduct a Data Protection Impact Assessment (DPIA) and implement appropriate technical and organisational measures, including pseudonymisation, and, where feasible, anonymisation, privacy-enhancing technologies, and comprehensive logging.
- » **Facilitate controlled data sharing for the purpose of scientific research.** Registered data banks will be required to establish data access committees and enter into binding agreements to release data only to vetted third-party researchers or public-sector bodies under strict safeguards, thereby streamlining national and cross-border collaboration.

5.8

Recognition of Research Ethics Committee – Mater Dei Hospital

Article 7 of the Data Protection Act makes special provision in relation to research concerning genetic data, biometric data or data concerning health in that the processing of such data for research purposes requires approval by the Commissioner on the advice of a Research Ethics Committee duly recognised for the same purpose. The Research Ethics Committee of Mater Dei Hospital (MDH) was formally recognised by the Commissioner, as the 'Research Health Ethics Committee' established under the auspices of the governance of MDH.

This formal recognition was provided following consultation meetings with MDH. As part of the request for such formal recognition, a data protection policy and terms of reference were developed by MDH and duly considered by the Commissioner. Other documents such as the information sheet template and the informed consent form template for both clinical and qualitative studies to be used in research projects were also reviewed. This was done in order to ensure proper processing by all parties involved.

By means of this formal recognition, the Research Ethics Committee of MDH was recognised as a committee having inter alia the oversight of medical and clinical research conducted at MDH, ensuring that all such activities are conducted

in compliance with both local and international regulatory requirements. This recognition was given subject to a number of conditions which include:

- » that the MDH Research Ethics Committee, in the evaluation of research proposals involving the processing of special categories of data, shall include within its structure a member having the necessary qualifications, skills and experience in the field of the protection of personal data;
- » that any research proposals are to be evaluated on the basis of the aforementioned documents submitted to the Commissioner for his consideration and that he may request any modifications to such documents in view of any requirements he may consider necessary to be introduced from time to time to the established procedure to ensure that the rights and freedoms of data subjects are safeguarded;
- » that recommendations in relation to applications for research concerning genetic data, biometric data or data concerning health for research purposes shall be forwarded to the Commissioner, requesting his authorisation in terms of the recommendations given.

5.9

Delivery of data protection lectures – Employment course – MEA

In line with its ongoing commitment to public awareness-raising and education, the office once again delivered a series of lectures during the year in collaboration with the Malta Employers' Association (MEA).

These sessions, aimed primarily at human resources personnel and employment-focused professionals, addressed the practical application of EU and domestic data protection law within the employment context. The IDPC provided guidance on key GDPR principles, including the lawful processing of employee personal data, the limitations of relying on consent due to power imbalances, and the

importance of identifying appropriate legal bases such as contractual necessity or legal obligations.

The lectures also covered transparency requirements, employee monitoring practices, handling of special categories of data, and data retention obligations, with a focus on ensuring compliance with the principles of necessity, proportionality, and data minimisation.

Overall, this initiative reflects the IDPC's continued efforts to support organisations through practical guidance and to enhance awareness of data protection rights and obligations in the workplace.

5.10

Proactive Engagement with Healthcare Providers on Data Protection Officer Requirements

During 2025, the office undertook a proactive initiative aimed at strengthening compliance within the healthcare sector in relation to the designation of Data Protection Officers (DPOs). In this regard, the Commissioner addressed a formal communication to healthcare providers, reminding them of their obligations under the GDPR concerning the mandatory designation and communication of DPO details.

Given the nature of their activities, healthcare providers routinely process special categories of personal data, particularly data concerning health. In line with article 37(1)(c) of the Regulation, where such processing is carried out on a large scale, the designation of a DPO

constitutes a legal obligation rather than a discretionary measure. The communication therefore emphasised the criteria for assessing 'large-scale' processing, including the number of data subjects affected, the volume and sensitivity of the data processed, the duration of processing activities and their geographical scope.

The office also highlighted the critical role of the DPO as a key component of an organisation's data protection governance framework. In particular, the DPO is responsible for advising controllers on their obligations, monitoring compliance and serving as a point of contact for both data subjects and the supervisory authority.

05

Our Initiatives and Engagements

5.10

Proactive Engagement with Healthcare Providers on Data Protection Officer Requirements

Healthcare providers were urged to review their internal practices and assess whether their processing activities trigger the obligation to appoint a DPO. Specific guidance was provided to distinguish between entities that are typically required to designate a DPO, such as hospitals and large clinics, and those that may not fall within the scope of large-scale processing, such as sole practitioners and small clinics.

Furthermore, the Commissioner reminded controllers of their obligation under article 37(7) of the Regulation to communicate the contact details

of the designated DPO to the office without undue delay and to ensure that such details are publicly accessible. Controllers were also informed of the potential consequences of non-compliance, including the possibility of corrective measures and administrative fines in accordance with article 83(4)(a) of the Regulation.

This initiative formed part of the office's broader strategy to promote awareness and ensure proactive compliance, particularly in sectors involving the processing of sensitive personal data.

5.11

Contributions to Privacy Laws and Business and MLex

During 2025, the office engaged with the publication Privacy Laws & Business (PL&B) as part of its ongoing efforts to contribute to international discourse on data protection and regulatory practice. Following discussions held at the GPA, representatives of PL&B visited Malta in April 2025 and conducted an in-depth interview with the Commissioner, together with members of the office.

The interview formed the basis of an article published in the PL&B International Report (June 2025 edition), which provided a comprehensive overview of Malta's data protection framework and the work of the office. The publication highlighted the office's organisational structure, its evolving role within the national regulatory landscape, and its increasing responsibilities, including its designation under the EU Artificial Intelligence Act.

The article also explored the office's approach to complaints handling and enforcement. It noted that all complaints

are treated with equal importance and are handled with a consistent level of diligence, irrespective of their nature. While certain complaints may be resolved within shorter timeframes, more complex cases are subject to detailed investigation and are typically concluded through legally binding decisions. The publication further referred to the office's focus on ensuring compliance through follow-up actions on decisions and corrective measures.

Particular attention was given to trends observed in complaint handling, including the significant volume of cases linked to the gaming sector and the continued increase in cross-border complaints. The article highlighted the office's role as Lead Supervisory Authority in a substantial number of such cases, reflecting Malta's position as a hub for digital and remote gaming services.

05

Our Initiatives and Engagements

5.11

Contributions to Privacy Laws and Business and MLex

The publication also addressed key legal developments and interpretative issues, including the application of restrictions to the right of access under national law and the importance of ensuring that any such limitations comply with the principles of necessity and proportionality. In addition, it reflected the office's position in relation to ongoing discussions at EU level on the potential simplification of certain GDPR obligations, particularly those relating to record-keeping requirements for small and medium-sized enterprises.

Furthermore, the article highlighted the office's efforts in promoting compliance and supporting organisations, including through advisory work and practical tools such as the GDPR self-assessment initiative aimed at assisting SMEs. It also referred to the office's cooperation with other supervisory authorities, both within the EDPB framework and through regional networks.

This engagement provided a valuable opportunity to present the work and priorities of the office within an international publication and to contribute to broader discussions on the practical application of data protection law. It also served to strengthen the office's visibility and engagement within the global data protection community.

During the year, the Commissioner was also interviewed by Matthew Newman of regulatory news portal MLex during the Privacy Symposium held in Venice. During the interview, Mr Deguara said that Malta's IDPC will be the market surveillance authority for the EU's AI Act. The IDPC, which is already in charge of fundamental rights under the AI Act, would be named as market surveillance authority on 2 August 2025 for certain high-risk AI systems.

To prepare for the two new roles, the authority is building up its expertise and will provide "comprehensive guidance," Deguara said

5.12

Publication of FAQs

During the year the office published a number of useful FAQs, namely on [Data Protection Officers \(DPOs\)](#), on [Management of Employee Email Accounts \(Post-Departure\)](#), and [Employment Sector](#).

06

Data Protection Regulatory Work



6.1

Contacts and Enquiries

Throughout 2025, the office continued to receive a significant number of enquiries from both individuals and organisations seeking guidance on a wide range of data protection matters. These enquiries were made through different channels, including via in-person visits to the IDPC's offices, telephone calls, as well as emails.

Email enquiries, in particular, continued to increase in 2025, with the IDPC receiving an average of approximately thirty-five (35) enquiries per week.

A large portion of enquiries pertained to the use of CCTV systems by individuals and organisations. Common questions concerned the legal considerations surrounding the installation and operation of CCTV, the appropriate placement of CCTV, the data protection rights of individuals captured by CCTV systems, and the use of specific technologies such as doorbell cameras and dashcams. Additional queries pertained to the retention periods for CCTV footage, the use of surveillance in sensitive environments, such as morgues and nursing homes, and the deployment of CCTV at the workplace.

Similarly, the IDPC received a notable amount of enquiries relating to the employment sector. These included questions about employee background checks being carried

out by employers, the limitations on accessing the electronic email accounts of employees, the use of work-issued mobile devices, the monitoring of employees' activity on such devices, and the handling of access requests made by employees to their employers.

In response to these recurring queries, the IDPC identified some of the most commonly asked questions and expanded its publicly available guidance by publishing dedicated FAQs on the employment sector, and updating its existing CCTV FAQs to better reflect commonly raised issues. These FAQs are accessible at the following links:

- » <https://idpc.org.mt/for-organisations/employment-sector/>
- » <https://idpc.org.mt/for-individuals/cctv/>

Other commonly asked questions included those pertaining to the exercise of right of access, the receiving of marketing and promotional communications, the unauthorised publication and dissemination of content on social platforms and online, questions pertaining to artificial intelligence and facial recognition, as well as the EU Data Act (Regulation (EU) 2023/2854), as well as general questions regarding the scope and applicability of the Regulation.

6.2

Advisory Services

Legislative Consultations in terms of article 36(4) of the GDPR

In 2025, a record number of proposed legislative measures were referred to this office for consultation, reflecting a significant increase in legislative measures involving the processing of personal data across a range of sectors. This demonstrates the growing recognition of data protection considerations and the importance of ensuring that legislative frameworks incorporate appropriate data protection safeguards, respect the principles of data protection, and uphold the fundamental right to the protection of personal data.

The Commissioner exercises this task pursuant to article 36(4) of the GDPR, which requires that the supervisory authority be consulted during the preparation of any legislative measure relating to the processing of personal data. During the reporting year, the Commissioner was consulted on the following legislative instruments:

- » The proposed bye-laws 'Use of Facilities (Tarxien Local Council) Bye-Laws', which, at the time of reporting had not yet been issued and published in the Government Gazette;
- » The proposed bye-laws 'Use of Facility and Administration of a Car Park Site, Malta Freeport Corporation, Birzebbuga (Birzebbuga Local Council) Bye-Laws', which, at the time of reporting had not yet been issued and published in the Government Gazette;
- » The amendments to the 'Company Service Providers (Exemption) Regulations', Subsidiary Legislation 529.02, introduced by virtue of Legal Notice 90 of 2025;
- » The amendments to the 'Markets in Crypto-Assets Act', Chapter 647 of the Laws of Malta, enacted by means of Act XI of 2025;
- » The proposed amendments to the 'Electronic Communications, the Single European Emergency Call Service (112" Number) and the European Harmonised Services of Social Value ("116" Numbering Range) Regulations', Subsidiary Legislation 399.47, which, at the time of reporting had not yet been issued and published in the Government Gazette;
- » Bill No. 145 – 'National Interest (Enabling Powers) Bill';
- » The proposed 'Voluntary and Not for Profit Organisations Act', which, at the time of reporting had not yet been presented to Parliament;
- » The 'Disciplinary Proceedings Regulations', Subsidiary Legislation 464.20, introduced by virtue of Legal Notice 248 of 2025;
- » The amendments to the 'Trusts and Trustees Act (Register of Beneficial Owners) (Amendment) Regulations', Subsidiary Legislation 331.10, introduced by virtue of Legal Notice 133 of 2025;
- » The proposed regulations the 'Movement of Soil Regulations' under the Agriculture Act, Chapter 639 of the Laws of Malta, which, at the time of reporting had not yet been issued and published in the Government Gazette;

6.2

Advisory Services

- » The proposed regulations the 'Vacant Properties Let to Tenants Residing in Residential Care for the Elderly Regulations' under the Housing Authority Act, Chapter 261 of the Laws of Malta, which, at the time of reporting had not yet been issued and published in the Government Gazette;
- » The regulations 'Data Protection (Fair Access to and Use of Data) Regulations', Subsidiary Legislation 586.13, introduced by virtue of Legal Notice 223 of 2025;
- » The regulations 'Artificial Intelligence (Designation of the Information and Data Protection Commissioner for the purposes of Regulation (EU) 2024/1689) Regulations', Subsidiary Legislation 586.14, introduced by virtue of Legal Notice 227 of 2025;
- » The proposed regulations the 'Data Protection (Research Exemption, Regulation of Processing of Personal Data for Scientific Research Purposes and Registration of Data Bank) Regulations' under the Data Protection Act, Chapter 586 of the Laws of Malta, which, at the time of reporting had not yet been issued and published in the Government Gazette;
- » The proposed amendments to the 'Processing of Personal Data (Secondary Processing) (Health Sector) (Amendment) Regulations', Subsidiary Legislation 528.10, which, at the time of reporting had not yet been issued and published in the Government Gazette;
- » The proposed amendments to the 'Restriction of the Data Protection Obligations and Rights) Regulations', Subsidiary Legislation 586.09, which at the time of reporting had not yet been issued and published in the Government Gazette;
- » The proposed amendments to the 'Traffic Regulation Ordinance', Chapter 65 of the Laws of Malta, which, at the time of reporting had not yet been issued and published in the Government Gazette;
- » The proposed amendments to the 'Gender-Based Violence and Domestic Violence Act', Chapter 581 of the Laws of Malta, which, at the time of reporting had not yet been presented to Parliament;
- » The proposed amendments to the 'Victims of Crime Act', Chapter 539 of the Laws of Malta, which, at the time of reporting had not yet been presented to Parliament;
- » The proposed regulations 'Drug-Driving Testing Regulations' under the Traffic Ordinance Act, Chapter 65 of the Laws of Malta, which, at the time of reporting had not yet been issued and published in the Government Gazette;
- » The regulations 'Online Dispensing of Medicinal Products to Third Countries from Free Zones and Customs Authorised Warehouses Regulations', introduced by virtue of Legal Notice 191 of 2025;
- » The proposed amendments to the 'Local Enforcement System (Establishment as an Agency) (Amendment) Order', Subsidiary Legislation 595.14, which, at the time of reporting had not yet been issued and published in the Government Gazette;

6.2

Advisory Services

- » The proposed regulations 'Investigation of Road Collisions and Safety Regulations' under the Authority for Transport in Malta Act, Chapter 499 of the Laws of Malta, which, at the time of reporting had not yet been issued and published in the Government Gazette;
- » The proposed amendments to the 'Malta Financial Services Authority (Amendment) Act', Chapter 330 of the Laws of Malta, which, at the time of reporting had not yet been presented to Parliament;
- » The regulations 'Miscarriage Leave Regulations' under the Employment and Industrial Relations Act, Chapter 452 of the Laws of Malta, which were introduced by virtue of Legal Notice 274 of 2025;
- » Bill No. 156 - 'Credit Review Office Act';
- » The proposed amendments to the 'Social Enterprise Act', Chapter 630 of the Laws of Malta, which, at the time of reporting had not yet been enacted;
- » The regulations 'Banking Act (Consumer Credit) (Amendment) Regulations', under the Banking Act, Chapter 371 of the Laws of Malta, introduced by virtue of Legal Notice 265 of 2025;
- » The proposed regulations the 'Financial Institutions Act (Consumer Credit) Regulations', under the Financial Institutions Act, Chapter 376 of the Laws of Malta, introduced by virtue of Legal Notice 266 of 2025;
- » The proposed regulations the 'Consumer Credit (Admission) Regulations', under the Banking Act, Chapter 371 of the Laws of Malta, which, at the time of reporting had not yet been issued and published in the Government Gazette;
- » The proposed amendments to the bye-laws 'Use of Facilities (L-Imdina (Città Nobile) Local Council) Bye-Laws', which, at the time of reporting had not yet been issued and published in the Government Gazette;
- » The proposed bye-laws 'Use of Facilities and Administration (H'Attard Local Council) Bye-Laws', which, at the time of reporting had not yet been issued and published in the Government Gazette;
- » The proposed bye-laws 'Use of Facilities and Administration (Xewkija Local Council) Bye-Laws', which, at the time of reporting had not yet been issued and published in the Government Gazette; and
- » The proposed amendments to 'Cooperation with Other Jurisdictions on Tax Matter (Amendment) Regulations', Subsidiary Legislation 123.127, which, at the time of reporting had not yet been issued and published in the Government Gazette.

6.3

Complaints

6.3.1 Data Protection Complaints

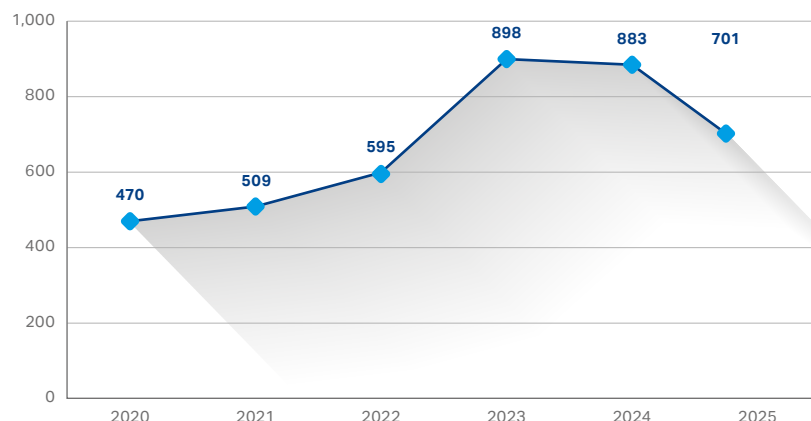
In 2025, the office received a total of seven hundred one (701) complaints, representing a decrease compared to the eight hundred eighty-three (883) complaints recorded in 2024. While this reflects a reduction in volume, the number of complaints remains relatively high when viewed in the context of previous years, indicating continued public awareness and engagement with data protection rights.

These complaints were processed through a structured case-handling system, resulting in a range of outcomes. By year-end, one hundred eighty-two (182) complaints were deemed admissible, one hundred thirty-one (131) remained under active investigation, one hundred forty-seven (147) were rejected, one hundred twenty-two (122) were dismissed, sixty-five (65) were classified as abandoned, thirty-three (33) were placed on hold, sixteen (16) were withdrawn, and five (5) were processed through the Internal Market Information (IMI) system.

At the initial stage of the complaints-handling process, all complaints undergo a structured pre-filtering assessment. This preliminary review is intended to ensure that each complaint contains the necessary information required for the office to proceed with an investigation.

A total of one hundred forty-seven (147) complaints were rejected at a preliminary stage. These were primarily due to procedural or jurisdictional issues. The most frequent reason for rejection during the reporting year was incorrect filing (54 cases). This typically arises where complaints are lodged against the incorrect controller, where the identity of the controller is not specified, or where the complaint is otherwise incorrectly directed. Another common ground for rejection was the absence of supporting evidence (20 cases). In such cases, complaints are submitted without the necessary evidence required to substantiate an alleged infringement of data protection law.

Annual Complaints



6.3

Complaints

Complaints received during 2025

IMI System	5
Withdrawn	16
Dismissed	122
Still being investigated	131
Rejected	147
Admissable	182
Abandoned	65
On Hold	33



6.3.1 Data Protection Complaints

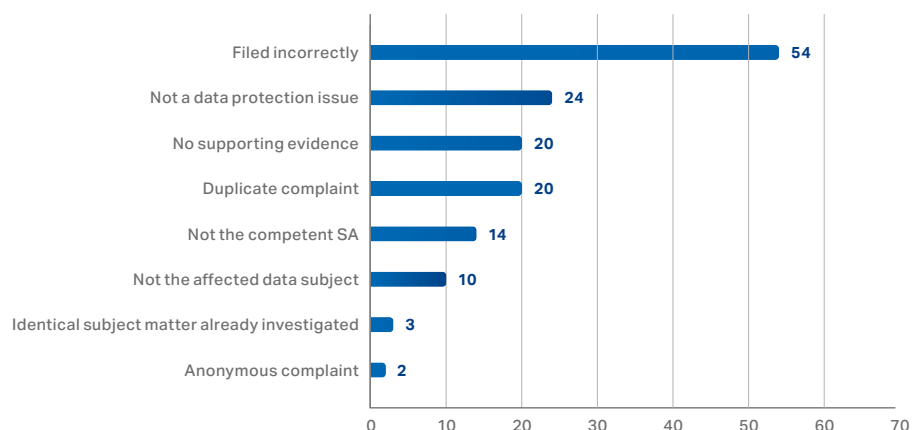
Other grounds for rejection included cases were rejected because they did not concern a data protection issue, others because they fell outside the competence of the supervisory authority, and in certain cases because the complainant was not the affected data subject.

Once a complaint passes the preliminary stage and the office proceeds to examine the merits of the case, it is no longer considered for rejection but may instead be dismissed following assessment. This distinction reflects the fact that the substance of the complaint is evaluated, including the factual background and the applicability of data protection law. The reasons for dismissal may vary. These include, among others, cases where the household exemption applies, where the complaint is considered unfounded or excessive, or where no infringement is identified following assessment. The most common

ground for dismissal during 2025, however, was that the office provided guidance to the data subject (60 cases). This typically arises in situations where a complaint is submitted prematurely or without first following the appropriate procedural steps.

For example, complaints are often lodged in relation to the exercise of data subject rights before the time period stipulated under article 12(3) of the Regulation has elapsed. In other instances, a data subject may submit a complaint without first exercising their rights directly with the controller. In such cases, the office does not proceed with a formal investigation but instead guides the data subject accordingly, informing them of the correct procedural steps to follow. This approach ensures that complaints are handled efficiently while also promoting a better understanding of data protection rights and obligations among the public. Twenty-six (26) cases were closed on the basis that no infringement was identified at that stage.

Rejected Complaints



06

Data Protection Regulatory Work

6.3

Complaints

6.3.1 Data Protection Complaints

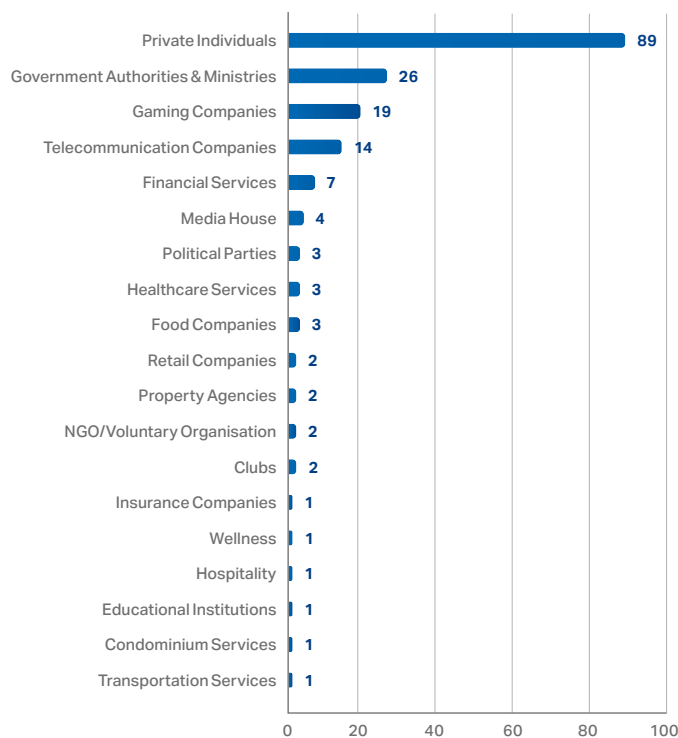
Sixty-five (65) complaints were classified as abandoned, typically due to a lack of engagement from complainants or failure to provide the necessary supporting documentation

within the stipulated timeframe.

Sixteen (16) complaints were formally withdrawn by the data subjects.

Additionally, thirty-three (33) complaints were placed on hold, mainly due to ongoing legal or procedural considerations requiring deferral of investigation.

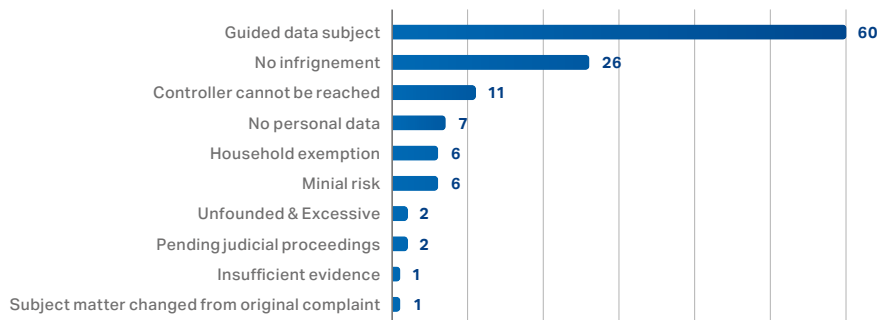
Admissible cases by Sector



Out of the total complaints received, one hundred eighty-two (182) were deemed admissible, having satisfied all legal requirements for investigation. These complaints originated from a wide range of sectors, with the largest proportion submitted by private individuals (89 cases). Other notable sectors included government authorities and ministries (26 cases), gaming companies (19 cases) and telecommunications companies (14 cases), alongside smaller contributions from financial services, media, healthcare and other industries.

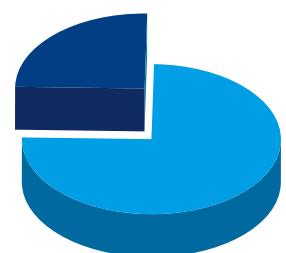
A total of one hundred eighty-two (182) admissible complaints were assessed, of which one hundred thirty-six (136) resulted in findings of infringement and forty-six (46) did not reveal any breach of data protection law. This reflects a relatively high rate of substantiated complaints.

Dismissed Complaints



Infringement 75%

No Infringement 25%



6.3

Complaints

6.3.1 Data Protection Complaints

In terms of subject matter, the most common issues raised in admissible complaints were related to CCTV (65 cases), data processing principles (33 cases) and data subject rights (50 cases). Other recurring issues included unauthorised disclosure (16 cases) and unauthorised access (4 cases).

In terms of the nature of complaints received, the most invoked data subject right was the right of access under article 15 of the Regulation. At the same time, the most frequently implicated principle was that of lawfulness, fairness and transparency, as set out in article 5(1)(a) of the Regulation. These trends indicate that a significant number of complaints continue to arise from issues relating to transparency of processing and the ability of data subjects to effectively exercise their rights. This pattern is consistent with the trends observed in 2024, where the right of access was likewise among the most frequently raised issues.

The infringements identified spanned multiple provisions of the Regulation and national legislation. The most frequently breached provisions included article 5(1) of the Regulation (principles relating to processing of personal data), infringed in thirty-two (32) cases, and article

6(1) of the Regulation (lawfulness of processing), infringed in twenty-eight (28) cases. Data subject rights also featured prominently, particularly article 15 of the Regulation (right of access), infringed in eleven (11) cases, and article 12(3) of the Regulation, relating to response timeframes, infringed in ten (10) cases. Several decisions involved multiple infringements.

In response to the infringements identified, the Commissioner adopted a range of corrective measures in accordance with article 58(2) of the Regulation. A commonly applied measure was the issuance of orders pursuant to article 58(2)(c) of the Regulation, particularly in cases involving failures to comply with data subject rights. Emphasis was placed on failures to respond to requests, especially subject access requests, within the legally prescribed timeframe. This issue was notably prevalent within the gaming sector, where controllers repeatedly failed to respond in a timely manner. In such cases, the Commissioner required controllers to provide evidence demonstrating that the request had been duly addressed and that access had been granted. Where no such evidence was submitted, the Commissioner issued a formal order requiring the controller to comply without further delay.



The most frequently breached provisions included article 5(1) of the Regulation (principles relating to processing of personal data), infringed in thirty-two (32) cases, and article 6(1) of the Regulation (lawfulness of processing), infringed in twenty-eight (28) cases.

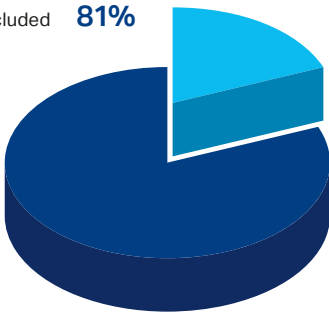


6.3

Complaints

Cases not concluded in 2025

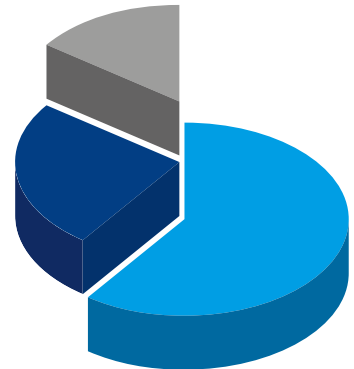
Still being investigated **19%**
Concluded **81%**

**6.3.1 Data Protection Complaints**

Orders pursuant to article 58(2)(d) of the Regulation were also frequently issued, particularly in relation to the improper deployment of CCTV systems. In several cases, CCTV cameras were found to be positioned in a manner that captured public areas or neighbouring private property, in breach of the principle of data minimisation. In such instances, the Commissioner ordered controllers to reconfigure their systems, typically by adjusting the angle of view of the cameras, to ensure that surveillance was strictly limited to areas within their own premises and proportionate to the intended purpose.

CCTV-related complaints continued to represent a significant portion of the office's workload. Out of sixty-five (65) admissible CCTV cases, thirty-nine (39) resulted in orders requiring the adjustment of camera angles to ensure that surveillance was limited to appropriate areas, while sixteen (16) resulted in orders for the removal of cameras altogether. Ten (10) cases were found not to involve any infringement.

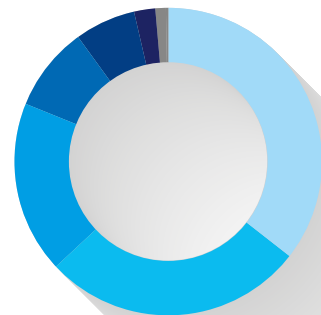
Order to adjust **60%**
Order to remove **25%**
No Infringement **15%**



In addition to these corrective measures, a number of cases were resolved through amicable settlements, whereby controllers took the necessary steps to remedy the identified shortcomings without the need for further enforcement action. This approach contributed to the efficient resolution of certain complaints while ensuring that data subjects' rights were effectively upheld.

By the end of the reporting year, one hundred thirty-one (131) complaints remained under active investigation and will be carried forward into the following year.

Direct Marketing: **2**
Unauthorised Access: **4**
Other: **12**
Unauthorised Disclosure: **16**
Data Protection Principles: **33**
Data Protection Rights: **50**
CCTV: **65**



6.3

Complaints

6.3.2 Summaries of Key Data Protection Cases

This section outlines a number of key data protection decisions issued by the IDPC in 2025. These legally binding decisions address crucial data protection issues, including the rights of data subjects, the obligations of controllers, the security of processing of personal data, and the enforcement action taken by the Commissioner in the event of non-compliance with the applicable laws.

The importance of the principle of data minimisation

This case concerned a complaint lodged against a service provider (the 'controller'), alleging that users were being forced to disclose their mobile numbers when paying bills owed to the controller through a particular online banking platform on which the controller had made itself available for the purpose of receiving bill payments.

“ The complainant argued that the controller would not allow payments to be processed unless this data field was filled in, notwithstanding that providing a mobile number was not considered necessary to process the payments. ”

The complainant argued that the controller would not allow payments to be processed unless this data field was filled in, notwithstanding that providing a mobile number was not considered necessary to process the

payments. The complainant therefore argued that the compulsory collection of this personal data was excessive and in breach of the Regulation.

During the course of the Commissioner's investigation, it was established that the controller had failed to demonstrate that collecting users' mobile numbers with every transaction was strictly necessary. The controller's stated purpose of the processing, namely, to contact data subjects in the event of erroneous or suspicious payments, were considered exceptional, and could be achieved through less intrusive means, such as by using the existing contact details held on the controller's systems. Therefore, the Commissioner determined that the controller had failed to comply with the principle of data minimisation under article 5(1)(c) of the Regulation.

Additionally, the controller had repeatedly failed to respond to the Commissioner's requests for submissions, which unnecessarily prolonged the investigation. Accordingly, it was also determined that the controller had infringed its obligation to cooperate with the supervisory authority, as required under article 31 of the Regulation.

The controller was issued with a reprimand and was ordered to bring its processing operations into compliance with the Regulation, by either removing the mobile number field on the payment form entirely or by making it optional. The controller was ordered to confirm its compliance no later than twenty days from the date of the decision and was warned that non-compliance would lead to an administrative fine. The controller complied, and ultimately modified the data field, making it optional.

6.3

Complaints

6.3.2 Summaries of Key
Data Protection Cases*Unlawful Processing and Disclosure of
Personal Data by a Healthcare Provider*

The Commissioner received a complaint from a data subject alleging that a controller had unlawfully processed and disclosed her personal data. In particular, the complainant stated that the controller had failed to update her residential address despite prior interactions, which resulted in correspondence containing sensitive health data being sent to an incorrect address and consequently disclosed to third parties. The complainant further questioned how the controller had obtained her personal data, noting that she had no prior relationship with the organisation.

During the course of the investigation, it was established that the controller had collected the complainant's personal data from the Electoral Register. However, the controller failed to identify a valid legal basis for such processing and did not provide the complainant with the information required under article 14 of the Regulation regarding the source and use of her personal data. This constituted a breach of the principles of lawfulness, fairness and transparency as set out in article 5(1) (a), as well as infringements of article 6(1) and article 14 of the Regulation.

The investigation also revealed that, despite being notified on multiple occasions of the inaccuracy of the complainant's address, the controller failed to rectify the data without undue delay. This failure resulted in the continued processing and

“ The investigation also revealed that, despite being notified on multiple occasions of the inaccuracy of the complainant's address, the controller failed to rectify the data without undue delay. ”

disclosure of inaccurate personal data, in breach of article 16 of the Regulation. Moreover, the controller did not take reasonable steps to ensure that personal data held was accurate and kept up to date, as required by article 5(1)(d) of the Regulation.

In addition, it was established that the controller operates as a healthcare provider and processes special category data on a large scale. In such circumstances, the controller was required to appoint a Data Protection Officer in accordance with article 37(1) (c) of the Regulation. The failure to appoint a DPO constituted a further infringement of the Regulation.

In light of the above findings, the Commissioner issued a reprimand pursuant to article 58(2)(b) of the Regulation in relation to the unlawful processing of personal data obtained from a publicly available source, the failure to rectify inaccurate data in a timely manner and the failure to comply with the requirement to appoint a DPO. Furthermore, corrective measures were imposed under article 58(2)(d), ordering the controller to rectify the complainant's personal data without undue delay, to erase all personal data that had been unlawfully obtained from the Electoral Register and to appoint a DPO in line with its obligations under the Regulation.

6.3

Complaints

6.3.2 Summaries of Key Data Protection Cases

Unlawful Processing and Disclosure of Personal Data by a Healthcare Provider

Additionally, the Commissioner imposed administrative fines under article 58(2) (i) of the Regulation, amounting to a total of €20,000. These included a fine of €12,500 for breaches relating to lawfulness, transparency and information obligations; a fine of €5,000 for the failure to comply with the right to rectification; and a fine of €2,500 for the failure to appoint a DPO.

Disclosure of ex-client personal data by their lawyer

The Commissioner received a complaint concerning an ex-client of a lawyer alleging that the latter, in his capacity as a data controller, unlawfully disclosed her personal data – including personal data the lawyer obtained during their client-lawyer relationship – to her employer.

During the investigations, the Commissioner noted that there had been an ongoing dispute between the two following the legal representation services provided by the lawyer involving

contestation by the complainant that the legal fees paid to the controller be returned. According to submissions received in the investigation, the complainant asserted that she would proceed to lodge a complaint/make a report with all concerned authorities against the controller on the basis of the complainant's assertion of improper tax/fiscal related practices, by the controller, in his capacity as her lawyer.

It transpired that the complainant worked within premises which included a department operated by the public tax authority. In the context of this dispute, the Commissioner observed that the complainant informed the controller that she sees him often, when passing through these premises, and moreover, she never hid the fact that she works in the tax system. The controller submitted he was aware that the premises referred to by the complainant in her communications to him, housed the concerned tax offices, and hence the place where she was employed.

The Commissioner observed that the controller expressed serious concern that, in the context of the dispute, the complainant could potentially, or may have already, used her position at her workplace - which information pertaining to her employment was publicly available on her LinkedIn profile - to unlawfully access his personal data for purposes unrelated to her employment. Once that was submitted, it was for this reason he had a legitimate interest to process certain personal data relating to her, for the purposes of making a report with the public tax regulator, being her employer.



The Commissioner received a complaint concerning an ex-client of a lawyer alleging that the latter, in his capacity as a data controller, unlawfully disclosed her personal data – including personal data the lawyer obtained during their client-lawyer relationship – to her employer.



6.3

Complaints

6.3.2 Summaries of Key
Data Protection CasesDisclosure of ex-client personal
data by their lawyer

The Commissioner was of the view that, while the complainant had every right to exercise all the remedies provided by law in relation to the dispute against the controller, the controller equally had the right to safeguard his personal data and request a verification from the complainant's employer, the tax regulator, as to whether his personal data was unlawfully accessed by the complainant for her own personal reasons.

In these circumstances, the controller's actions to safeguard his legal interests, in particular his fundamental right to the protection of his personal data, and to prevent any potential unlawful processing of his personal data, indeed constituted a legitimate interest, provided in conformity with the rest of the principles of the GDPR.

“...the controller's actions to safeguard his legal interests, in particular his fundamental right to the protection of his personal data, and to prevent any potential unlawful processing of his personal data, indeed constituted a legitimate interest...”

In the Commissioner's assessment to determine whether the controller had lawfully disclosed the complainant's personal data, being his ex-client, to her employer, in the pursuit of such legitimate interest, the Commissioner assessed, amongst other things, the criteria deemed necessary to fulfil the legal basis of legitimate interest under article 6(1)(f) of the GDPR, and for this reason, the controller was requested to provide a copy of the legitimate interest assessment conducted prior to the disclosure of his ex-client's personal data.

The Commissioner consequently determined when evaluating the 'three-part test' of the basis of legitimate interest, that the controller was justified in disclosing to the tax regulator in the context of the report, basic identifiability details relating to the complainant, such as name, surname, and the branch she worked at. However, other information included, such as a private correspondence between them which did not convey supporting evidence relevant in the context of his report to the tax regulator, was deemed not necessary, and hence such additional information of a private nature was not covered by justification of a legitimate interest. For this reason, the Commissioner exercised his powers under article 58(2)(b) of the GDPR, thereby issuing the controller with a reprimand for exceeding the limits of the processing of personal data for the purposes of his report made.

6.4

Ex-Officio
Investigations

During the reporting period, the Commissioner conducted ex-officio investigations upon becoming aware of potential infringements of the data protection legislation that could affect the fundamental right to the protection of personal data. These investigations are part of the ongoing efforts to monitor the applicability of the law.

The negligent disposal of personal data, including special categories of personal data

The Commissioner became aware of media reports alleging that a controller had disposed of entire documents containing personal data, including special categories of personal data, by leaving them in waste bags on a pavement for collection by waste services. Some of the documents were reportedly scattered from open or partially open waste bags.

“ In consultation with another public authority, the Commissioner gathered sufficient information to ascertain that the waste bags did indeed contain documents with personal data, including special categories of personal data. ”

Following these reports, the Commissioner conducted a thorough investigation. In consultation with another public authority, the Commissioner gathered sufficient information to ascertain that the waste bags did indeed contain documents with personal data, including special categories of personal data.

In terms of article 5(1)(e) of the GDPR, the principle of storage minimisation requires that personal data should

not be retained for longer than necessary. Personal data that are no longer necessary for the purpose of the processing must be securely destroyed. For paper records, secure shredding is generally considered best practice, provided that documents are rendered into pieces small enough to exclude identification.

After reviewing the submissions of the controller and the evidence collected, the Commissioner concluded that the method of disposal used by the controller was not compliant with the data protection legislation. Once the documents were discarded in waste bags and left on a pavement, the controller failed to maintain the ongoing confidentiality of personal data through the whole lifecycle of the processing.

As a result, the Commissioner determined that the controller had disposed of documentation containing personal data, including special categories of personal data, in a negligent manner, therefore infringing article 5(1)(f) of the GDPR. In exercising his corrective powers, the Commissioner imposed an administrative fine pursuant to article 58(2)(i) of the GDPR. The controller appealed the decision.

This case demonstrates the importance of secure data disposal and highlights the Commissioner's commitment to enforcing the obligations of the controller across all stages of data processing, including disposal.

The security aspect of the distribution and collection of the identity documents

The Commissioner initiated an ex-officio investigation into the security aspect of the distribution and collection of identity

6.4

Ex-officio
Investigations

documents by the postal service. Upon investigation, the Commissioner raised serious concerns regarding this processing activity. Identity card documents are afforded heightened protection under law. Specifically, article 8 of the Data Protection Act, Chapter 586 of the Laws of Malta, imposes stringent obligations on any controller processing such documents. Moreover, identity documents contain biometric data, which, under article 9(1) of the GDPR, constitute a special category of personal data. This rendered the processing inherently high-risk.

Considering these significant data protection concerns and the potential risks to the rights and freedoms of the data subjects, the Commissioner ordered the controller to cease the

to processing of personal data as set forth in article 5(1)(f) of the GDPR. The controller complied with the decision.

Unlawful processing of personal data accessed from the Government's Common Database (CdB)

The Commissioner became aware of a potential infringement of the data protection legislation following the publication, in a newspaper, of a photograph showing a computer desktop screen containing the Government's Common Database. The image captured personal data of an identified individual.

Following consultations with another public authority and the collection of relevant information, the Commissioner established that the controller responsible for the infringement had accessed the personal data of the affected data subject for reasons completely unrelated to the tasks of a public officer.

The Commissioner concluded that the controller accessed the personal data, captured a photograph of the screen showing the database, and subsequently, disclosed the data to an unauthorised third party. By virtue of article 58(2)(b) of the GDPR, the Commissioner reprimanded the controller for having infringed the principle of lawfulness in terms of article 5(1)(a), including article 6(1) of the GDPR. The decision has become final, as no appeal was lodged.

“ Considering these significant data protection concerns and the potential risks to the rights and freedoms of the data subjects, the Commissioner ordered the controller to cease the processing operation pursuant to article 58(2)(f) of the GDPR. ”

processing operation pursuant to article 58(2)(f) of the GDPR. The controller was also instructed to explore alternative methods for delivery and distribution of identity documents that fully comply with the GDPR, including the principles relating

06

Data Protection Regulatory Work

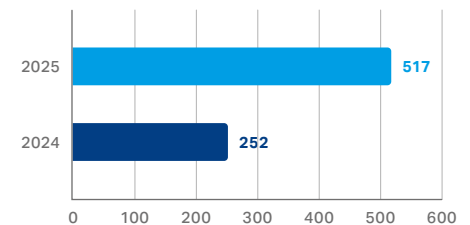
6.5

One-Stop-Shop Cases

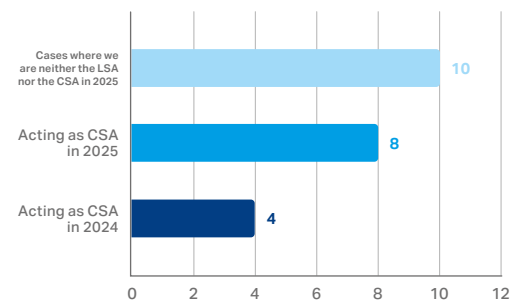
In 2025, there were five hundred and thirty-five (535) complaints filed under the Internal Market Information (IMI) system, a substantial increase compared to the two hundred and fifty-six (256) complaints recorded in 2024. Out of these, five hundred and seventeen (517) were LSA cases, and eight (8) were CSA cases, compared to two hundred and fifty-two (252) and four (4) cases respectively in the previous year. In 2025, the IDPC has also been wrongly identified as LSA in ten (10) cases where, after a preliminary investigation, it was established that we were neither the LSA or the CSA.

It appeared that this is due to either wrong information on the controllers' websites or wrong interpretation of such information by the transferring SA.

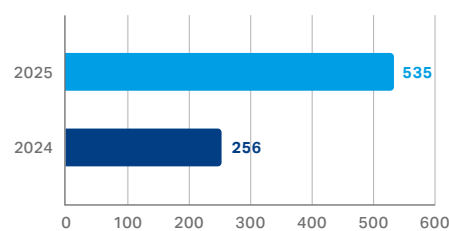
Cases acting as LSA



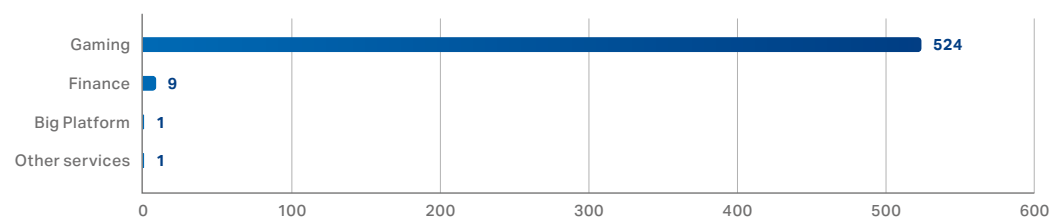
Cases where we were not the LSA



Total OSS Cases



Number of Complaints by Sector

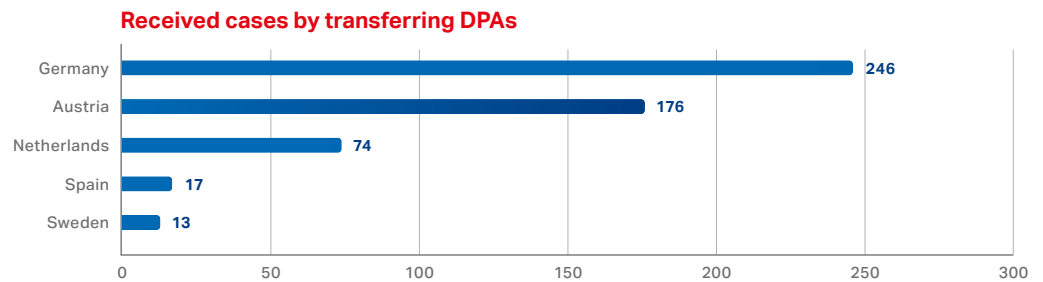


06

Data Protection Regulatory Work

6.5

One-Stop-Shop Cases



The majority of cases were received from Germany (246), followed by Austria (176), the Netherlands (74), Spain and Sweden receiving respectively 17 and 13 and other countries receiving fewer cases.

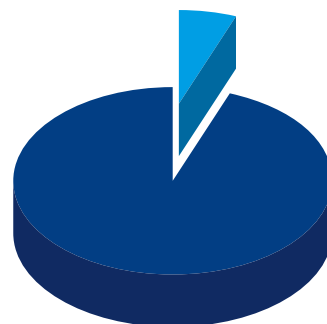
Most of these complaints, four hundred and fifty (450) cases, were related to right of access requests, followed by under tens of case of identity theft, right of erasure requests, security of processing and transparency.

Regarding case outcomes, five hundred and five (505) complaints were deemed admissible, eight (8) were withdrawn either by the complainants or the CSA and twenty-two (22) were closed.

Most of the investigation are pending, waiting for the outcome of appeals for similar cases at a national level.

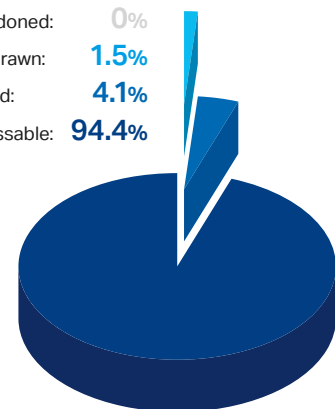
Number of Cases

Completed: **30**
Pending: **505**



Complaint Status

Dismissed: **0%**
Abandoned: **0%**
Withdrawn: **1.5%**
Closed: **4.1%**
Admissible: **94.4%**



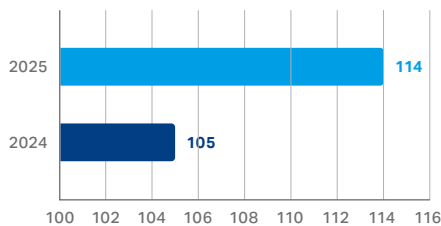
06

Data Protection Regulatory Work

6.6

Personal Data Breaches

Total breaches reported



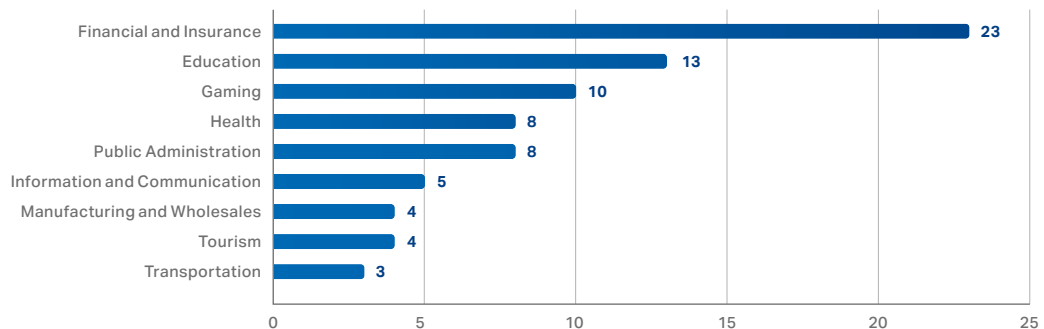
In 2025, a total of one hundred and fourteen (114) personal data breaches were reported, marking an increase from the one hundred and five (105) breaches reported in 2024.

The sectors most affected by these breaches is the financial sector which included insurance company as well with twenty-three (23) incidents reported followed by education with thirteen (13) breached, gaming with ten (10), health and public administration with 8 (eight), information and communication with five (5).

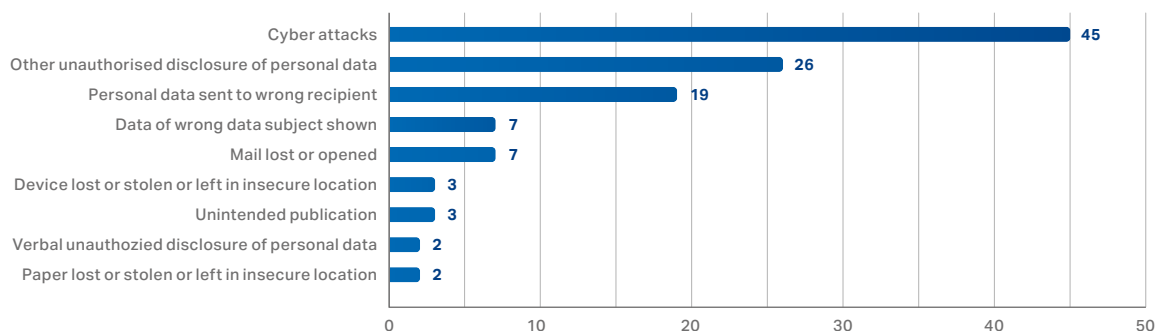
Lesser affected sectors included manufacturing and tourism with four (4) and transportation with three (3) reported breaches. Nine (9) notifications were withdrawn by the controllers.

The majority of the breaches had as cause cyberattacks, including phishing attacks and ransomware attacks, which accounted for forty-five (45) incidents. Other causes were unauthorised disclosure of personal data personal (26 breaches), data of wrong data subject shown (19 breaches), mail lost or opened and data of wrong data subject shown (7 breaches respectively).

Number of breaches by sector



Nature of the breaches



6.6

Personal Data Breaches

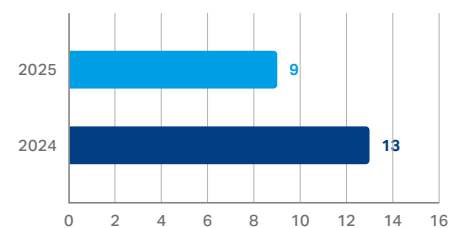
Less common causes were unintended publication and device lost or stolen or left in insecure location and paper lost or stolen or left in insecure location and verbal unauthorised disclosure of personal data with respectively 3 and 2 reported breaches.

In terms of notifications received from controllers outside the EU, there was a slightly decrease from thirteen (13) in 2024 to nine (9) in 2025.

Throughout the year, the number of breaches reported fluctuated, peaking in June with thirteen (13) breaches reported.

Investigations are ongoing.

Number of notified breaches by controllers outside the EU



6.7

Administrative Fine imposed by the Commissioner

During the year 2025, the Commissioner concluded an investigation following a complaint concerning the unlawful processing and disclosure of personal data by a controller. The investigation established multiple infringements of the Regulation, including breaches of the principles of lawfulness and transparency, failure to ensure data accuracy, non-compliance with data subject rights, and the absence of a required Data Protection Officer.

In accordance with article 58(2)(i) of the GDPR, the Commissioner imposed three (3) administrative fines amounting to €20,000. Further details on this case are provided under section 6.3.2 of this report – “Summary of Cases”.



In accordance with article 58(2)(i) of the GDPR, the Commissioner imposed three (3) administrative fines amounting to €20,000. ”

6.8

Supervisory Audits

The European Union continues to operate a number of large-scale IT systems designed to facilitate cooperation and information exchange between member states in areas such as border management, migration, law enforcement, customs, and the functioning of the internal market. Key systems include Eurodac, the Visa Information System (VIS), the Schengen Information System (SIS), the Customs Information System (CIS), and the Internal Market Information System (IMI). These databases enable competent authorities across the EU to exchange information efficiently and support the effective implementation of EU policies.

Given the large volume of personal data processed by these systems, strong supervisory mechanisms remain essential. Supervision is therefore shared between national Data Protection Authorities (DPAs) and the European Data Protection Supervisor (EDPS). National DPAs oversee the use of these systems at the national level, ensuring that authorities within their jurisdiction comply with applicable data protection rules. At the same time, the EDPS supervises the operation and management of the systems at the EU institutional level.

To ensure a high and consistent level of data protection across the Union, national DPAs through their national supervisory function and the EDPS continue to cooperate closely in the coordinated supervision of these large-scale databases. This collaboration is particularly significant for systems related to police and judicial cooperation, where sensitive personal data may be processed. Through coordinated oversight activities, regular exchanges of expertise, and joint supervisory

efforts, the authorities work together to ensure that these systems operate in full compliance with EU data protection standards and uphold the fundamental rights of individuals.

On-site Inspections and Audits – 2025

Pursuant to article 55 of the Regulation (EU) 2018/1861 and article 41 of Regulation (EU) 2021/1134, the office, in its capacity as the national supervisory authority, is responsible for monitoring the lawfulness of the processing of personal data carried out at national level within the Schengen Information System (SIS) and the Visa Information System (VIS).

For the purpose of effectively carrying out the tasks assigned to this office by law, during the reporting period, this office conducted a series of on-site inspections and audits within the Malta Police Force to assess compliance with applicable data protection requirements in the operation of large-scale EU information systems at national level. These inspections were carried out at the SIRENE bureau, N.SIS unit, Europol National Central Bureau (NCB), Eurodac national office and the Passenger Name Record (PNR) unit.

In the last quarter of 2025, this office also carried out an onsite inspection related to the implementation of the Entry Exit System (EES) in Malta. The EES, which became operational on the 12 October 2025, is an automated IT system used to register the entry and exit data of non-EU nationals travelling for short stays each time they cross the external border of the twenty-nine (29) European countries using the system.

6.8

Supervisory Audits

In 2025, this office also conducted on-site inspections in relation to the processing and issuance of short-stay visas. These were carried out at the Visa Office within the Ministry for Foreign Affairs and Tourism, Identità and the High Commission of Malta in London.

Further audits and onsite inspections were carried out at the Commerce Department in relation to the supervision of the processing of personal data in the Internal Market Information System (IMI) in accordance with Article 21 of Regulation (EU) No 1024/2012 (as modified by Article 38 of Regulation (EU) 2018/1724), the national European Public Prosecutor's Office (EPPO) the supervision of the processing of operational personal data in the context of cooperation between the national members within the EPPO in accordance with Article 87 of Regulation (EU) 2017/1939, and the European Union Agency for Criminal Justice Cooperation (Eurojust) in the supervision of the processing of operational personal data in the context of cooperation between the national members within Eurojust in accordance with Article 42(2) of Regulation (EU) 2018/1727.

Schengen Evaluation and Monitoring Mechanism

Under the Schengen evaluation and monitoring mechanism, and in particular, pursuant to article 18 of Regulation (EU) 2022/922, the European Commission maintains a pool of experts from Member States to ensure the availability of a sufficient number

of experts to conduct evaluation or monitoring activity in relation to the Schengen Information System (SIS).

The office contributed to the pool of experts by nominating representatives in the field of data protection. In May 2025, experts from the IDPC were selected to participate in the Data Protection Schengen Evaluation of Slovenia.

During the same year, a member of the office was selected by the European Commission to participate in a team of auditors for the purpose of carrying out the Schengen Evaluation Verification visit to Cyprus, which took place in November 2025.

Coordinated Supervision Committee

The Coordinated Supervision Committee (CSC) is composed of representatives of the national supervisory authorities and the EDPS. It ensures coordinated supervision of large-scale IT systems, as well as those systems of certain EU bodies, offices and agencies, in accordance with article 62 of Regulation (EU) 2018/1725. This office actively participates in this forum, and representatives of the IDPC, SA attended the CSC meetings on a regular basis.

As of 2025, the CSC has been entrusted with addressing data protection arising in the context of coordinated supervision related to Internal Market Information System (IMI), the European Union Agency for Criminal Justice Cooperation (Eurojust), the European Public Prosecutor's Office (EPPO), and the Entry-Exit System (EES).

6.8

Supervisory Audits

Number of requests submitted by data subjects during year 2025 to exercise their data protection rights pursuant to regulation 17 of Subsidiary Legislation 586.08

Schengen Information System II (SIS II)

Completed Access Requests	Alert on the data subject under Regulation (EU) 2018/1860	Alert on the data subject under Regulation (EU) 2018/1861	Alert on the data subject under Regulation (EU) 2018/1862	No alert on the applicant in the Schengen Information System (SIS)	Total
Subject Access Requests	12	51	2	72	137
Completed Erasure Requests	0	1	0	0	1
Total number of requests:					138

Passenger Name Record (PNR)

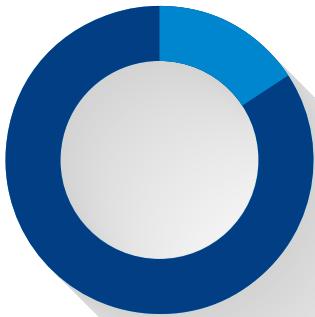
In accordance with article 13(2) of the Passenger Name Record (Data) (Chapter 584 of the Laws of Malta), upon expiry of six (6) months from the date of transfer of the PNR data, all such data must be depersonalised through masking. However, where it is demonstrated that access to the full PNR data is necessary for the purposes of the prevention, detection, investigation or prosecution of terrorist offences and serious crime, the Data

Protection Officer of the National Passenger Information Unit (NPIU) may request the Commissioner in writing to approve the unmasking and disclosure of the full PNR data, in accordance with article 13(3)(b)(ii) of the Act.

During the reporting period, the Commissioner received a total of eighty-one (81) requests for approval pursuant to article 13(3) of the Act.

07

Freedom of Information

2025 Workload (667)

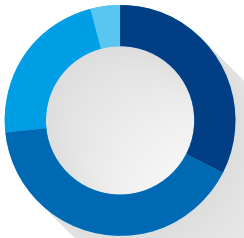
Cases opened in 2024
but closed in 2025: **18%**

New cases Recorded in 2025 **82%**

A total of six hundred sixty-seven (667) cases were handled by public authorities during the reporting period. This figure includes one hundred eighteen (118) cases that were opened in 2024 and carried forward into 2025, as well as five hundred forty-nine (549) new requests recorded during 2025.

Out of the five hundred forty-nine (549) new requests received in 2025, one hundred sixty-three (163) were accepted, one hundred twenty-two (122) were refused, two hundred forty-eight (248) remained pending by year-end, and sixteen (16) were withdrawn. With respect to the one hundred eighteen (118) cases carried forward from 2024, thirty-eight (38) were accepted, twenty-six (26) were refused, forty-seven (47) remained pending, and seven (7) were withdrawn.

The Lands Authority received the highest number of requests, totalling one hundred eighty-one (181). Of these, eight (8) were accepted, sixteen (16) were refused, one hundred fifty-three (153) remained pending, and four (4) were withdrawn. The Malta Police Force recorded the second highest number of requests, with twenty-eight (28) cases, of which seventeen (17) were accepted, seven (7) were refused, and four (4) remained pending.

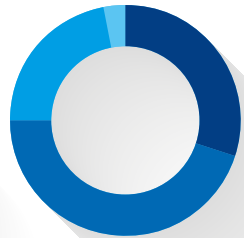
**Public Authorities
– 2024 Cases**

Withdrawn: **6%**

Still being processed: **22%**

Not accepted: **40%**

Accepted: **32%**

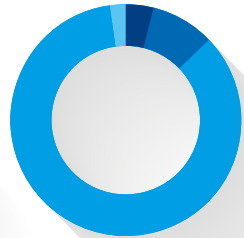
**Public Authorities
– 2025 Cases**

Withdrawn: **3%**

Still being processed: **22%**

Not accepted: **45%**

Accepted: **30%**

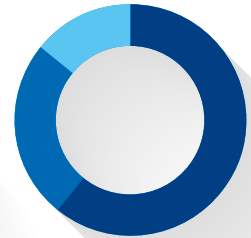
Lands Authority (181 total)

Withdrawn: **2%**

Still being processed: **85%**

Not accepted: **9%**

Accepted: **4%**

Malta Police Force (28 total)

Withdrawn: **0%**

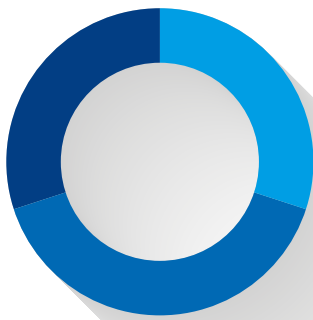
Still being processed: **14%**

Not accepted: **25%**

Accepted: **61%**

Public authorities relied on a number of legal grounds when refusing access to documents. The most frequently cited reason was classified under “other reasons” (78 cases). Among the specified grounds, the most common included cases where the document requested was not held by the public authority or was more closely connected with the functions of another authority (18 cases), as well as other reasons which are highlighted below:

Reason for Requests refused	Total
Document is withheld in terms of Part V or Part VI of the Act.	16
Document requested is excluded from the scope of the Freedom of Information Act by virtue of Article 5.	8
Other reasons	78
Resources required to identify, locate or collate the document or documents would substantially and unreasonably divert the resources of the authority for its operations.	2
The information relating to a decision or recommendation requested pursuant to article 20 of the Act is being withheld in terms of Part V or VI of the said Act.	2
The document requested is not held by the Public Authority, or connected more closely with the functions of, another public authority.	18
The document requested is publicly available or will be published within three months.	17
The request is considered frivolous, trivial or vexatious.	1
The document requested cannot be found and this is certified in writing by the head of the public authority	6
	148

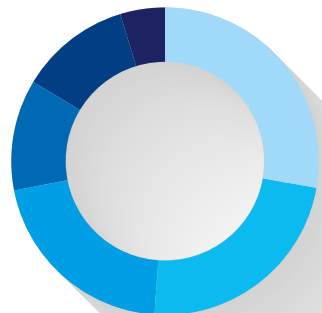
Decision Notices

Justified: 3
Not justified: 4
Partially justified: 3

The office received a total of fifty-two (52) FOI applications during 2025. Out of these, forty-three (43) were concluded during the reporting year, while nine (9) remained ongoing and were carried forward into the following year. The cases carried forward represent applications for which the assessment or investigation could not be finalised within the same reporting period and will therefore continue to be handled in 2026. Of the applications concluded, five (5) were dismissed and two (2) were withdrawn. A number of cases were resolved through cooperative measures, including twelve (12) amicable settlements and five (5)

cases which were resolved through a combination of an information notice and amicable settlement. In addition, nine (9) enforcement notices were issued.

The Commissioner issued a total of ten (10) Decision Notices. In three (3) cases, the exemption invoked by the public authority was found to be justified; in four (4) cases, it was found not to be justified; and in three (3) cases, it was found to be partially justified. One (1) case has been taken to appeal.



5% Withdrawn
12% Information Notice and Amicable Settlement
11% Dismissed
21% Enforcement Notice
23% Decision Notice
28% Amicable Settlement

08

Financial Statements



Office of the Information and Data Protection Commissioner

Annual Report and Financial Statements

For the Year Ended 31 December 2025

Office of the Information and Data Protection Commissioner
For the Year Ended 31 December 2025
Contents

	<u>Page(s)</u>
Commissioner's Report	1 - 2
Independent Auditor's Report	3 - 4
Statements of Comprehensive Income	5
Statement of Financial Position	6
Statement of Changes in Equity	7
Statement of Cash Flows	8
Notes to the Financial Statements	9 - 21

Office of the Information and Data Protection Commissioner

Commissioner's Report

For the Year Ended 31 December 2025

The Commissioner presents this report and the audited financial statements of the Office of the Information and Data Protection Commissioner (hereinafter referred to as "the Authority") for the year ended 31 December 2025.

General Information

The Office of the Information and Data Protection Commissioner was set up by the Data Protection Act, Cap. 440 of the Laws of Malta, which came into force on 22 March 2002. As of 28 May 2018, this Act was replaced by Chapter 586 (the "Act").

Principal Activities

The principal activity of the Office of the Information and Data Protection Commissioner is to ensure respect for the individual's right to privacy with regard to personal information, which constitutes the fundamental pursuits for every democratic society and to administer the provisions of the Freedom of Information Act.

Review of Business Development and State of Affairs

The Authority's main source of income is from the subvention received from the Government of Malta amounting to €800,000 (2024: €750,000) for the year ended 31 December 2025 which is utilised to cover recurrent expenditure. Total administrative expenditure amounted to €811,880, resulting in an increase of 15% when compared to 2024. As a result, the Authority incurred a deficit of €4,530 for the year ended 31 December 2025 compared to surplus €49,720 from the previous year.

As from 1 January 2016, the Government and the Authority have agreed that notification fees received by the Authority, and any administrative fines shall be reimbursed back to the Government. This agreement remains in force as at today. As from 25 May 2018, operators no longer have the obligation to pay notification fees to the Authority. In 2025, the Authority did not collect any notification fees (2024: Nil).

Going concern

The Authority registered a deficit of €4,530 during the year under review (2024: surplus €49,720). The Authority anticipates that current services will continue to be provided with full support from the Government of Malta. For this reason, the Authority does not foresee a significant impact on its operational performance. Therefore, the financial statements have been prepared on the going concern basis which assumes that the Authority will continue in operational existence for the foreseeable future and that adequate support will continue to be made available by the Government of Malta through the subventions to enable the Authority to meet its commitments as and when they fall due.

Financial Risk Management

For principal risks and uncertainties, refer to Note 2.m., 'Financial Risk Management', of the financial statements that provides details in connection with the Authority's key risks factors including liquidity risk, foreign exchange risk, fair values risk and capital risk management and the Authority's approach towards managing these risks.

Events after the balance sheet date

No significant events have occurred after the balance sheet date which require mention in this report.

Future Developments

The Authority is not envisaging any changes in operating activities for the forthcoming year.

Office of the Information and Data Protection Commissioner

Commissioner's Report (continued)

For the Year Ended 31 December 2025

Commissioner

The Commissioner who held office during the year was:

Mr. Ian Deguara (resigned on 23 April 2026)

Mr. Reno Borg (appointed on 24 April 2026)

In accordance with article 11 of the Data Protection Act, CAP. 586 of the Laws of Malta, the Commissioner was appointed by the Prime Minister after having consulted with the Leader of the Opposition. The Commissioner was appointed for a period of five years, with effect from 24 April 2026.

The present Commissioner shall continue in office.

Statement of the Commissioner's responsibilities for the financial statements

The Commissioner is required to prepare financial statements that give a true and fair view of the financial position of the Authority as at the end of each reporting period and of the surplus or deficit for that year.

In preparing the financial statements, the Commissioner is responsible for:

- ensuring that the financial statements have been drawn up in accordance with International Financial Reporting Standards ("IFRS") as adopted by the European Union ("EU");
- selecting and applying appropriate accounting policies;
- making accounting estimates that are reasonable in the circumstances; and
- ensuring that the financial statements are prepared on the going concern basis unless it is inappropriate to presume that the Authority will continue in business as a going concern.

The Commissioner is also responsible for designing, implementing and maintaining internal control as the Commissioner determines is necessary to enable the preparation of financial statements that are free from material misstatement, whether due to fraud or error. The Commissioner is also responsible for safeguarding the assets of the Authority and hence for taking reasonable steps for the prevention and detection of fraud and other irregularities.

Auditors

PKF Malta Limited, Registered Auditors, have expressed their willingness to continue in office and a resolution for their reappointment will be proposed at the Annual General Meeting.

Approved by the Commissioner on 10 August 2026 and signed by:

Reno Borg
Commissioner

Registered Address:

Floor 2, Airways House
High Street
Sliema SLM 1549
Malta

Independent Auditor's Report

To the Commissioner of the Office of the Information and Data Protection Commissioner

Report on the audit of the financial statements

Opinion

We have audited the accompanying financial statements of the Office of the Information and Data Protection Commissioner set out on pages 5 to 21 which comprise the statement of financial position as at 31 December 2025, the statements of comprehensive Income, statement of changes in equity and statement of cash flows for the year then ended, and notes to the financial statements, including a summary of material accounting policies and other explanatory information.

In our opinion, the accompanying financial statements give a true and fair view of the financial position of the Authority as at 31 December 2025, and of its financial performance and its cash flow for the year then ended in accordance with International Financial Reporting Standards (IFRS) as adopted by the European Union (EU) and have been properly prepared in accordance with the requirements of the Data Protection Act (Cap. 586) (the "Act").

Basis for Opinion

We conducted our audit in accordance with International Standards on Auditing (ISAs). Our responsibilities under those standards are further described in the Auditor's Responsibilities for the Audit of the Financial Statements section of our report. We are independent of the Authority in accordance with the International Ethics Standards Board for Accountants' Code of Ethics for Professional Accountants (IESBA Code) together with the ethical requirements that are relevant to our audit of the financial statements in accordance with the Accountancy Profession (Code of Ethics for Warrant Holders) Directive issued in terms of the Accountancy Profession Act (Cap. 281) in Malta, and we have fulfilled our other ethical responsibilities in accordance with these requirements and the IESBA Code. We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Other Information

The Commissioner is responsible for the other information. The other information comprises the information included in the annual report, other than the financial statements and our auditor's report thereon.

Our opinion on the financial statements does not cover the other information and we do not express any form of assurance conclusion thereon other than our reporting on other legal and regulatory requirements.

In connection with our audit of the financial statements, our responsibility is to read the other information and, in doing so, consider whether the other information is materially inconsistent with the financial statements or our knowledge obtained in the audit, or otherwise appears to be materially misstated. If, based on the work we have performed, we conclude that there is a material misstatement of this other information, we are required to report that fact. We have nothing to report in this regard.

Responsibilities of the Commissioner

The Commissioner is responsible for the preparation of the financial statements that (i) give a true and fair view in accordance with IFRS as adopted by the EU, (ii) are properly prepared in accordance with the provisions of the Act, and (iii) for such internal control as the Commissioner determines is necessary to enable the preparation of financial statements that are free from material misstatement, whether due to fraud or error.

In preparing the financial statements, the Commissioner is responsible for assessing the Authority's ability to continue as a going concern, disclosing, as applicable, matters related to going concern and using the going concern basis of accounting unless the Commissioner either intends to liquidate the Authority or to cease operations, or has no realistic alternative but to do so.

Auditor's Responsibilities for the Audit of the Financial Statements

Our objectives are to obtain reasonable assurance about whether the financial statements as a whole are free from material misstatement, whether due to fraud or error, and to issue an auditors' report that includes our opinion. Reasonable assurance is a high level of assurance, but is not a guarantee that an audit conducted in accordance with ISAs will always detect a material misstatement when it exists. Misstatements can arise from fraud or error and are considered material if, individually or in the aggregate, they could reasonably be expected to influence the economic decisions of users taken on the basis of these financial statements.

Independent Auditor's Report (continued)

To the Commissioner of the Office of the Information and Data Protection Commissioner

Auditor's Responsibilities for the Audit of the Financial Statements (continued)

As part of an audit in accordance with ISAs, we exercise professional judgment and maintain professional scepticism throughout the audit. We also:

- Identify and assess the risks of material misstatement of the financial statements, whether due to fraud or error, design and perform audit procedures responsive to those risks, and obtain audit evidence that is sufficient and appropriate to provide a basis for our opinion. The risk of not detecting a material misstatement resulting from fraud is higher than for one resulting from error, as fraud may involve collusion, forgery, intentional omissions, misrepresentations, or the override of internal control.
- Obtain an understanding of internal control relevant to the audit in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the Authority's internal control.
- Evaluate the appropriateness of accounting policies used and the reasonableness of accounting estimates and related disclosures made by the Commissioner.
- Conclude on the appropriateness of the Commissioner's use of the going concern basis of accounting and based on the audit evidence obtained, whether a material uncertainty exists related to events or conditions that may cast significant doubt on the Authority's ability to continue as a going concern. If we conclude that a material uncertainty exists, we are required to draw attention in our auditors' report to the related disclosures in the financial statements or, if such disclosures are inadequate, to modify our opinion. Our conclusions are based on the audit evidence obtained up to the date of our auditor's report. However, future events or conditions may cause the Authority to cease to continue as a going concern.
- Evaluate the overall presentation, structure and content of the financial statements, including the disclosures, and whether the financial statements represent the underlying transactions and events in a manner that achieves fair presentation.

We communicate with the Commissioner regarding, among other matters, the planned scope and timing of the audit and significant audit findings, including any significant deficiencies in internal control that we identify during our audit.

The principal in charge of the audit resulting in this independent auditor's report is Mr. George Mangion for and on behalf of:

PKF Malta Limited
Registered Auditors

15, Levels 3, Mannarino Road
Birkirkara BKR 9080
Malta

10 August 2026

Office of the Information and Data Protection Commissioner

Statements of Comprehensive Income

For the Year Ended 31 December 2025

		2025	2024
	Note	€	€
Government subvention	4.	800,000	750,000
Administrative expenses		(811,880)	(704,500)
Operating (loss)/surplus		(11,880)	45,500
Other income		15,000	13,000
Finance costs	5.	(7,650)	(8,541)
Loss on disposal		-	(239)
(Deficit)/surplus for the year		(4,530)	49,720

The notes on pages 9 to 21 form an integral part of these financial statements.

Office of the Information and Data Protection Commissioner

Statement of Financial Position

As at 31 December 2025

	Note	2025 €	2024 €
ASSETS			
Non-current assets			
Property, plant and equipment	9.	215,718	251,442
Intangible assets	10.	7,522	-
Total non-current assets		223,240	251,442
Current assets			
Other receivables	11.	3,621	1,581
Cash and cash equivalents	12.	297,896	300,485
Total current assets		301,517	302,066
TOTAL ASSETS		524,757	553,508
EQUITY AND LIABILITIES			
Equity			
Retained Funds	13.	195,853	200,383
Liabilities			
Non-current liabilities			
Lease liabilities	14.	209,809	236,659
Current liabilities			
Lease liabilities	14.	26,749	26,749
Trade and other payables	15.	92,346	89,717
Total current liabilities		119,095	116,466
TOTAL EQUITY AND LIABILITIES		524,757	553,508

The notes on pages 9 to 21 form an integral part of these financial statements.

These financial statements on pages 5 to 21 were approved by the Office of the Information and Data Protection Commissioner on 10 August 2026 and were signed on its behalf by:

Reno Borg
Commissioner

Office of the Information and Data Protection Commissioner

Statement of Changes in Equity

For the Year Ended 31 December 2025

	Retained Funds €	Total Equity €
Balance as at 01 January 2025	200,383	200,383
Loss for the year	(4,530)	(4,530)
Balance as at 31 December 2025	195,853	195,853

	Retained Funds €	Total Equity €
Balance as at 01 January 2024	150,663	150,663
Surplus for the year	49,720	49,720
Balance as at 31 December 2024	200,383	200,383

The notes on pages 9 to 21 form an integral part of these financial statements.

Office of the Information and Data Protection Commissioner

Statement of Cash Flows

For the Year Ended 31 December 2025

		2025	2024
	Note	€	€
Cash from operating activities:			
(Loss)/surplus for the year		(4,530)	49,720
Interest expense	14.	7,650	8,541
Depreciation of property, plant and equipment	9.	39,370	39,695
Loss on disposal of property, plant and equipment		-	239
Amortisation of intangible assets	10.	2,508	-
Profit from operations		44,998	98,195
Movement in trade and other receivables		(2,040)	9
Movement in trade and other payables		2,629	(24,436)
Net cash flows from operating activities		45,587	73,768
Cash flows from investing activities:			
Payments for property, plant and equipment	9.	(3,646)	(1,498)
Disposal of property, plant and equipment		-	200
Payments to acquire intangible assets	10.	(10,030)	-
Net cash flows used in investing activities		(13,676)	(1,298)
Cash flows from financing activities:			
Repayment of finance lease liabilities	14.	(34,500)	(34,500)
Net cash flows used in financing activities		(34,500)	(34,500)
Net cash (used in)/from cash and cash equivalents		(2,589)	37,970
Cash and cash equivalents at beginning of year		300,485	262,515
Cash and cash equivalents at end of year	12.	297,896	300,485

The notes on pages 9 to 21 form an integral part of these financial statements.

1. Basis of Preparation

a. Statement of compliance

The financial statements have been prepared and presented in accordance with the requirements of the International Financial Reporting Standards ("IFRS") as adopted by the European Union ("EU"). They have also been drawn up in accordance with the provisions of the Data Protection Act Cap. 586 of Laws of Malta (the "Act").

b. Basis of measurement

The financial statements have been prepared on the historical cost basis.

c. Functional and presentation currency

The financial statements are presented in euro (€), which is the Authority's functional currency.

d. Use of estimates and assumptions

The preparation of financial statements in conformity with IFRSs as adopted by the EU requires management to make judgments, estimates and assumptions that affect the application of accounting policies and the reported amounts of assets, liabilities, income and expenses. Actual results may differ from these estimates.

Estimates and underlying assumptions are reviewed on an ongoing basis. Revisions to accounting estimates are recognised in the period in which the estimates are revised and in any future periods affected.

e. Changes in accounting policies and disclosures

Standards, interpretations and amendments to published standards as endorsed by the EU effective in the current year

In the current year, the Authority adopted amendments and interpretations to existing standards that are mandatory to the Authority's accounting period beginning from 1 January 2025. The adoption of these revisions to the requirements of IFRSs as adopted by the EU did not result in substantial changes to the Authority's accounting policies.

Standards, interpretations and amendments to published standards as endorsed by the EU that are not yet effective

Certain new standards, amendments and interpretations to existing standards have been published by the date of authorisation for issue of these financial statements that are not yet effective.

The Authority has not early adopted these revisions to the requirements of IFRSs as adopted by the EU and the Commissioner is of the opinion that there are no requirements that will have a possible significant impact on the Authority's current or future reporting periods and on foreseeable future transactions.

f. Going concern

The financial statements have been prepared on the going concern basis which assumes that the Authority will continue in operational existence for the foreseeable future and that adequate support will continue to be provided by the Government of Malta through the subventions to enable the Authority to meet its obligations as they fall due.

2. Material Accounting Policies

a. Right of use asset

A right-of-use asset is recognised at the commencement date of a lease. The right-of-use asset is measured at cost, which comprises the initial amount of the lease liability, adjusted for, as applicable, any lease payments made at or before the commencement date net of any lease incentives received, any initial direct costs incurred, and, except where included in the cost of inventories, an estimate of costs expected to be incurred for dismantling and removing the underlying asset, and restoring the site or asset.

Right-of-use assets are depreciated on a straight-line basis over the unexpired period of the lease or the estimated useful life of the asset, whichever is the shorter. Where the Authority expects to obtain ownership of the leased asset at the end of the lease term, the depreciation is over its estimated useful life. Right-of use assets are subject to impairment or adjusted for any remeasurement of lease liabilities.

At the termination of a lease, the right-of-use asset and associated lease liability are removed from the books of the lessee. The difference between the two amounts is accounted for as a profit or loss at that time.

b. Property, plant and equipment

i. Recognition and measurement

Property, plant and equipment are initially recognised at cost. These are subsequently stated at cost less accumulated depreciation and accumulated impairment losses.

Cost includes expenditure that is directly attributable to the acquisition of the asset and any other costs directly attributable to bringing the assets to a working condition for their intended use, and the costs of dismantling and removing the items and restoring the site on which they are located.

ii. Depreciation

Depreciation is charged to the statement of comprehensive income on a straight-line basis over the estimated useful lives of items of property, plant and equipment, and major components are accounted for separately. The estimated useful lives are as follows:

Leased buildings	11 years
Furniture and fixtures	10%
Motor vehicles	20%
Office equipment	15%
Air conditioners	25%

Gains and losses on the disposal or retirement of an item of property, plant and equipment are determined as the difference between the net disposal proceeds and the carrying amount at the date of disposal. The gains or losses are recognised in the statement of comprehensive income as other operating income or other operating costs, respectively.

iii. Derecognition

Property, plant and equipment is derecognised and removed from the statement of financial position on disposal or when no future economic benefits are expected. Gains and losses from derecognition are measured as the difference between the net disposal proceeds, if any, and the carrying amount and are recognised in the statement of comprehensive income in the period of recognition.

2. Material Accounting Policies (Continued)

c. Intangible assets

i. Recognition and measurement

An intangible asset is recognised only if it is probable that the expected future economic benefits that are attributable to the asset will flow to the entity and the cost of the asset can be measured reliably. An intangible asset is initially measured at cost, comprising its purchase price and any directly attributable cost of preparing the asset for its intended use.

Intangible assets are subsequently carried at cost less any accumulated amortisation and any accumulated impairment losses.

ii. Derecognition of intangible assets

Intangible assets are derecognised on disposal or when no future economic benefits are expected from their use or disposal. Gains and losses arising from derecognition represent the difference between the net proceeds, if any, and the carrying amount and are included in profit or loss in the period of derecognition.

iii. Amortisation

Amortisation is calculated to write down the carrying amount of the intangible asset using the straight-line method over its expected useful life. Amortisation of an asset begins when it is available for use and ceases at the earlier of the date that the asset is classified as held for sale or the date that the asset is derecognised. Amortisation is charged to the statement of comprehensive income on a straight-line basis over the estimated useful lives of intangible assets. The estimated useful life for intangibles with definite lives are as follows:

Computer software	4 years
-------------------	---------

The useful lives of the intangible assets are reviewed on an annual basis and the useful life is altered if appropriate.

d. Impairment of non-financial assets

The carrying amount of the Authority's non-financial assets are reviewed at each reporting date to determine whether there is any indication of impairment. If such indication exists, then the asset's recoverable amount is estimated.

An impairment loss is recognised if the carrying amount of an asset or its cash-generating unit exceeds its recoverable amount. A cash-generating unit is the smallest identifiable group that generates cash flows that largely are independent from other assets and groups. Impairment losses are recognised in profit or loss.

The recoverable amount of an asset or cash-generating unit is the greater of its value in use and its fair value less cost to sell. In assessing value in use, the estimated future cash flows are discounted to their present value using a pre-tax discount rate that reflects current market assessments of the time value of money and the risks specific to the asset.

Impairment losses recognised in prior periods are assessed at each reporting date for any indications that the loss has decreased or no longer exists. An impairment loss is reversed if there has been a change in the estimates used to determine the recoverable amount. An impairment loss is reversed only to the extent that the asset's carrying amount does not exceed the carrying amount that would have been determined, net of depreciation or amortisation, if no impairment loss had been recognised.

2. Material Accounting Policies (Continued)

e. Financial instruments

i. Recognition and derecognition

Financial assets and financial liabilities are recognised when the Authority becomes a party to the contractual provisions of the financial instrument.

Financial assets are derecognised when the contractual rights to the cash flows from the financial asset expire, or when the financial asset and substantially all the risks and rewards are transferred. A financial liability is derecognised when it is extinguished, discharged, cancelled or expires.

ii. Classification and initial measurement of financial assets

The Authority recognises a financial asset in its statement of financial position when it becomes a party to the contractual provisions of the instrument. At initial recognition, the Authority measures a financial asset at its fair value plus, in the case of a financial asset not at fair value through profit or loss (FVPL), transaction costs that are directly attributable to the acquisition of the financial asset.

Financial assets, other than those designated and effective as hedging instruments, are classified into the following categories:

- amortised cost;
- fair value through profit or loss (FVTPL); or
- fair value through other comprehensive income (FVOCI)

In the period presented, the Authority does not have any financial assets categorised as FVPTL and FVOCI.

The classification is determined by both:

- the entity's business model for managing the financial asset; and
- the contractual cash flow characteristics of the financial asset.

iii. Subsequent measurement of financial assets

Financial assets are measured at amortised cost if the assets meet the following conditions (and are not designated as FVTPL):

- they are held within a business model whose objective is to hold the financial assets and collect its contractual cash flows; and
- the contractual terms of the financial assets give rise to cash flows that are solely payments of principal and interest on the principal amount outstanding.

After initial recognition, these are measured at amortised cost using the effective interest method. Discounting is omitted where the effect of discounting is immaterial. The Authority's cash and cash equivalents and receivables fall into this category of financial instruments.

2. Material Accounting Policies (Continued)

e. Financial instruments (Continued)

iv. Impairment of financial assets

IFRS 9's impairment requirements are based on forward-looking information to recognise expected credit losses (ECL), referred to as the 'ECL model'.

The Authority considers a broader range of information when assessing credit risk and measuring ECLs, including past events, current conditions, reasonable and supportable forecasts that affect the expected collectability of the future cash flows of the instrument.

In applying this forward-looking approach, a distinction is made between:

- financial instruments that have not deteriorated significantly in credit quality since initial recognition or that have low credit risk ('Stage 1') and

- financial instruments that have deteriorated significantly in credit quality since initial recognition and whose credit risk is not low ('Stage 2').

'Stage 3' would cover financial assets that have objective evidence of impairment at the reporting date.

'12-month ECLs' are recognised for the first category while 'lifetime ECLs' are recognised for the second category. The Authority measures its receivables and bank balances at the 12-month ECLs.

v. Classification and measurement of financial liabilities

The Authority's financial liabilities include trade and other payables and provisions. Financial liabilities are initially measured at fair value, and, where applicable, adjusted for transaction costs unless the Authority designated a financial liability at FVTPL.

Subsequently, financial liabilities are measured at amortised cost using the effective interest method except for derivatives and financial liabilities designated at FVTPL, which are carried subsequently at fair value with gains or losses recognised in profit or loss (other than derivative financial instruments that are designated and effective as hedging instruments).

All Interest-related charges and changes in an instrument's fair value (if applicable) are recognised as finance costs in the statement of income and expenditure.

vi. Derecognition

A financial liability is derecognised when the obligation under the liability is discharged or cancelled or expires. When an existing financial liability is replaced by another from the same lender on substantially different terms, or the terms of an existing liability are substantially modified, such an exchange or modification is treated as the recognition of the original liability and the recognition of a new liability. The difference in the respective carrying amounts is recognised in the statement of profit or loss.

vii. Offsetting

Financial assets and financial liabilities are offset, and the net amount presented in the statement of financial position if there is a currently enforceable legal right to offset the recognised amounts and there is an intention to settle on a net basis, to realise the assets and settle the liabilities simultaneously.

2. Material Accounting Policies (Continued)

f. Other receivables

Other receivables comprise of prepayments. Prepayments are recognised initially at cost when the payment is made. They are subsequently expensed in profit or loss on a systematic basis over the period to which the related goods or services pertain.

g. Cash and cash equivalents

Cash and cash equivalents comprise of cash in hand and bank balances. Cash equivalents are short-term investments that are held to meet short-term cash commitments rather than for investment or other purposes.

h. Provisions and contingent liabilities

Provisions are recognised when the Authority has a present obligation (legal or constructive) as a result of a past event, it is probable that the Authority will be required to settle that obligation and a reliable estimate can be made of the amount of the obligation. The amount recognised as a provision is the best estimate of the consideration required to settle the present obligation at the reporting date, taking into account the risks and uncertainties surrounding the obligation. Where a provision is measured using the cash flows estimated to settle the present obligation, its carrying amount is the present value of those cash flows (when the effect of the time value of money is material). When some or all of the economic benefits required to settle a provision are expected to be recovered from a third party, a receivable is recognised as an asset if it is virtually certain that reimbursement will be received and the amount of the receivable can be measured reliably.

A contingent liability is disclosed where the existence of the obligation will only be confirmed by future events or where the amount of the obligation cannot be measured with sufficient reliability.

i. Lease liabilities

A lease liability is recognised at the commencement date of a lease. The lease liability is initially recognised at the present value of the lease payments to be made over the term of the lease, discounted using the interest rate implicit in the lease or, if that rate cannot be readily determined, the Authority's incremental borrowing rate. The lessee's incremental borrowing rate applied to the lease liabilities is 3%.

Lease payments comprise of fixed payments less any lease incentives receivable, variable lease payments that depend on an index or a rate, amounts expected to be paid under residual value guarantees, exercise price of a purchase option when the exercise of the option is reasonably certain to occur, and any anticipated termination penalties. The variable lease payments that do not depend on an index or a rate are expensed in the period in which they are incurred.

Lease liabilities are measured at amortised cost using the effective interest method. The carrying amounts are remeasured if there is a change in the following: future lease payments arising from a change in an index or a rate used; residual guarantee; lease term; certainty of a purchase option and termination penalties. When a lease liability is remeasured, an adjustment is made to the corresponding right-of use asset, or to profit or loss if the carrying amount of the right-of-use asset is fully written down.

Lease payments on short-term leases and leases of low-value assets are recognised as an expenses on a straight-line basis over the lease term.

j. Trade and other payables

Trade and other payables comprise obligations to pay for goods or services that have been acquired in the ordinary course of business from suppliers. Accounts payable are classified as current liabilities if payment is due within one year or less (or in the normal operating cycle of the business, if longer). If not, they are presented as non-current liabilities.

2. Material Accounting Policies (Continued)

k. Government grant

The Authority is funded by Government grants which are voted separately for recurrent expenditure. Grants from the government are recognised at their fair value where there is reasonable assurance that the grant will be received and that the Authority will comply with all attached conditions. Government grants relating to costs are deferred and recognised in the Statement of Comprehensive Income over the period necessary to match them with the costs that they are intended to compensate. When the grant relates to an asset, it is recognised as income in equal amounts over the expected useful life of the related asset.

l. Foreign currencies

Transactions denominated in currencies other than the functional currency are translated at the exchange rates ruling on the date of transaction. Monetary assets and liabilities denominated in currencies other than the functional currency are re-translated to the functional currency at the exchange rate ruling at year end. Exchange differences arising on the settlement and on the retranslation of monetary items are dealt with in profit or loss.

m. Employee benefits

The Authority contributes towards the state pension in accordance with local legislation. The only obligation of the Authority is to make the required contributions. Costs are expensed in the period in which they are incurred.

n. Financial risk management

The Authority's activities expose it to a variety of financial risks: market risk (including currency risk, fair value interest rate risk and price risk), credit risk, liquidity risk and cash flow interest rate risk. The Authority's overall risk management program focuses on the unpredictability of financial markets and seeks to minimise potential adverse effects on the Authority's financial performance.

i. Market risk

Foreign exchange risk

Foreign exchange risk refers to the risk that the value of a financial commitment or recognised asset or liability will fluctuate due to changes in foreign currency rates. The Authority is exposed to foreign exchange risk arising from various currency exposure, primarily with respect to the Euro.

Foreign exchange risk arises from future commercial transactions, recognised assets and liabilities and net investments in foreign operations. The Authority monitors its foreign currency exposure on an ongoing basis.

ii. Liquidity risk

The Authority is exposed to liquidity risk in relation to meeting future obligations associated with its financial liabilities, which comprise lease liabilities (Note 14) and trade and other payables (Note 15). Prudent liquidity risk management includes maintaining sufficient cash and committed credit lines to ensure the availability of an adequate amount of funding to meet the Authority's obligations.

The Authority monitors and manages its risk to a shortage of funds by maintaining sufficient cash and by monitoring the availability of raising funds to meet commitments associated with financial instruments and by maintaining adequate banking facilities to meet the Authority's obligations when they become due.

Notes to the Financial Statements (Continued)

For the Year Ended 31 December 2025

2. Material Accounting Policies (Continued)

n. Financial risk management (Continued)

iii. Fair values

The fair values of financial assets and liabilities were not materially different from their carrying amounts as at year end.

iv. Capital risk management

The Authority's objectives when managing capital are to safeguard its ability to continue as a going concern. The capital structure of the Authority consists of cash and cash equivalents as disclosed in note 12. and items presented within the retained funds in the statement of financial position.

3. Judgements in applying accounting policies and key sources of estimation uncertainty

The preparation of the Authority's financial statements requires management to make judgements, estimates and assumptions that affect the reported amounts of revenues, expenses, assets and liabilities and the accompanying disclosures, and the disclosures of contingent liabilities. Uncertainty about these assumptions and estimates could result in outcomes that require a material adjustment to the carrying amount of assets or liabilities affected in future periods.

Estimates and assumptions

The Commissioner has assessed that there are no key assumptions or sources of estimation uncertainty that are likely to result in material adjustments to the carrying amounts of assets and liabilities within the next financial year. The Authority based its assumptions and estimates on parameters available when the financial statements were prepared. Existing circumstances and assumptions about future developments, however, may change due to market changes or circumstances arising that are beyond the control of the Authority. Such changes are reflected in the assumptions when they occur.

Judgements

The Commissioner has concluded that there were no significant judgements made in the application of accounting policies that would significantly affect the amounts recognised in the financial statements.

4. Government subvention

The Authority is funded by Government grants which are voted separately for recurrent expenditure.

	2025	2024
	€	€
Government subvention	800,000	750,000

5. Finance costs

	2025	2024
	€	€
Lease Finance costs	7,650	8,541

Office of the Information and Data Protection Commissioner

Notes to the Financial Statements (Continued)

For the Year Ended 31 December 2025

6. (Deficit)/surplus for the year

(Deficit)/surplus for the year is charged after charging the following:

	2025	2024
	€	€
Auditor's remuneration	2,891	2,750
Depreciation and amortisation	41,878	39,695
Total	44,769	42,445

7. Taxation

In accordance with the official tax exemption letter received from the Ministry of Finance and Employment, the Office of the Information and Data Protection is exempt from the payment of income tax in terms of Article 12(2) of the Income Tax (Cap. 123) of the Laws of Malta. Accordingly, the Authority did not provide for tax at 35% in these financial statements.

8. Staff costs

a. Wages and salaries

Payroll costs for the year comprise of the following:

	2025	2024
	€	€
Salaries and wages	569,000	465,989
Social security contributions	34,031	29,650
Total	603,031	495,639

b. Number of employees

The average number of persons employed by the Authority during the year was as follows:

	2025	2024
	No.	No.
Commissioner	1	1
Operational staff	12	10
Total	13	11

Notes to the Financial Statements (Continued)

For the Year Ended 31 December 2025

9. Property, plant and equipment

	Right-of-use assets	Furniture and fixtures	Motor vehicles	Office equipment	Air conditioners	Total
	€	€	€	€	€	€
Cost						
Opening balance	362,719	72,186	17,400	66,036	7,294	525,635
Additions	-	-	-	2,825	821	3,646
Disposals	-	-	(17,400)	-	-	(17,400)
Balance at 31 December 2025	362,719	72,186	-	68,861	8,115	511,881
Depreciation						
Opening balance	(131,898)	(56,439)	(17,400)	(62,720)	(5,736)	(274,193)
Charge for the year	(32,975)	(3,191)	-	(2,220)	(984)	(39,370)
Depreciation released on disposal	-	-	17,400	-	-	17,400
Balance at 31 December 2025	(164,873)	(59,630)	-	(64,940)	(6,720)	(296,163)
Carrying amount						
At 31 December 2024	230,821	15,747	-	3,316	1,558	251,442
At 31 December 2025	197,846	12,556	-	3,921	1,395	215,718

a. Right-of-use assets

Right-of-use assets represent the leased building which is currently being used as the registered office of the Office of the Information and Data Protection Commissioner. The lease agreement was entered into on 10 December 2020, effective from 1 January 2021 and is effective for a period of 11 years, of which the first 5 years will be *di fermo* and the last 6 years will be *di rispetto*.

10. Intangible Assets

	Computer software
	€
Cost	
Opening balance	25,038
Additions	10,030
Balance at 31 December 2025	35,068
Amortisation	
Opening balance	(25,038)
Amortisation	(2,508)
Balance at 31 December 2025	(27,546)
Carrying amount	
At 31 December 2024	-
At 31 December 2025	7,522

11. Other receivables

	2025	2024
	€	€
Prepayments	3,621	1,581

12. Cash and cash equivalents

Cash and cash equivalents for the purpose of the cash flow statement are as follows:

	2025	2024
	€	€
Cash on hand	585	427
Bank balances	297,311	300,058
Total cash and cash equivalents	297,896	300,485

13. Retained Funds

The retained fund represents accumulated surpluses carried forward.

14. Lease liabilities**a. Amounts recognised in the statement of financial position**

The statement of financial position shows the following amounts relating to leases:

	2025	2024
	€	€
Right-of-use assets		
Buildings	197,846	230,821
Lease liabilities		
Current	26,749	26,749
Non-current	209,809	236,659
Total	236,558	263,408

14. Lease liabilities (Continued)**a. Amounts recognised in the statement of financial position (Continued)**

The maturity of lease commitments is analysed as follows:

	2025	2024
	€	€
Less than one year	26,749	26,749
Between one and five years	135,762	127,843
More than five years	74,047	108,816
	236,558	263,408

b. Amounts recognised in the statements of comprehensive Income

Statements of comprehensive Income shows the following amounts relating to leases:

	2025	2024
	€	€
Depreciation of right-of-use assets	32,975	32,975
Interest expense	7,650	8,541

The total cash outflow of the Authority for leases during the year ended 31 December 2025 is €34,500 (2024: €34,500).

15. Trade and other payables

	2025	2024
	€	€
Trade payables	6,066	1,925
Accruals	5,233	6,745
Amount payable to related party (Note 17.)	81,047	81,047
Total	92,346	89,717

The amount payable to related party is due to the Government of Malta and is unsecured, interest free and repayable on demand.

16. Contingencies

The Authority holds a bank guarantee of €2,600 issued by Icon Studio in connection with service tender for the design, development, supply and maintenance of an online self-assessment compliance tool. The guarantee serves as security for the performance obligations under the agreement and as per initial terms it was valid until 1st July 2025, which was extended for a further period up to 30th July 2026. The guarantee is callable by the Authority in the event of non-performance or breach of contract by the counterparty. No amounts have been recognised in respect of this guarantee as at the year ended, as no default has occurred.

Office of the Information and Data Protection Commissioner

Notes to the Financial Statements (Continued)

For the Year Ended 31 December 2025

17. Related Party Transactions

The Authority is an independent public Authority and reports directly to the Parliament of Malta. It is free from external influence, whether direct or indirect, and does not take or seek instructions from any person or entity. Year end balances payable to related parties are disclosed in note 15.

18. Subsequent events

There were no subsequent events which would require an adjustment or disclosure in the financial statements of the Authority.

19. Statutory Information

The Office of the Information and Data Protection Commissioner is a government authority established in Malta.