2024

Annual Report
& Financial Statements

idpc. INFORMATION AND DATA PROTECTION COMMISSIONER

Contents

01

Key Performance Figures

01 Key Performance Figures

Complaints

883
Total Complaints Received

112
CCTV-related cases dominated the area of investigation

Article 6(1)
Most infringed GDPR Article

7
Ex-officio investigations

One Stop Shop Cases

256
Total OSS cases of which **244** relating to the gaming sector

252
Lead Supervisory Authority (LSA) cases

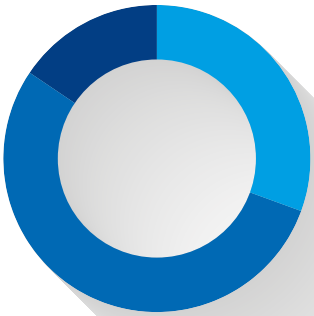
4
Concerned Supervisory Authority (CSA) cases

01

Key Performance Figures

Freedom of Information Applications

Decision notices issued:



Justified: 4
Not justified: 7
Partially justified: 2

798 Total Number of Requests received by Public Authorities

47 FOI Applications handled by IDPC

13 Resolved through amicable settlement between the parties

Data Breaches

105 Total breaches reported

21 Incidents reported by controllers in the education sector

61 Cyber-attacks including phishing and ransomware

02

Foreword

02

Foreword

I am pleased to present the annual report which covers the year 2024 - a year that once again underscored the vital importance of protecting personal data in a rapidly evolving digital world.

In 2024, we witnessed a significant increase in cross-border complaints, mainly relating to cases lodged with our European counterparts relating to the exercise of data protection rights with gaming operators having their main establishments in Malta.

We have also witnessed new challenges deriving primarily for the use of artificial intelligence. More than ever, our mandate remains resolute, that is to continue with our mission to uphold the fundamental rights of individuals, ensure accountability among data controllers and processors, and provide guidance that is practical, proportionate and rooted in law.

This past year, our office dealt with a growing number of data protection queries received from controllers operating in different sectors, and from individuals who either enquired about specific personal situations on which they required our professional feedback or otherwise about the exercise of their data protection rights. We can safely say that this increase in the number of engagement stems from an increase in public awareness of information rights.

During the year, it is with satisfaction to report that our office was requested to provide advice to the Government on several legislative measures concerning the protection of the rights and freedoms of natural persons in relation to the processing of personal data.

By virtue of this consultation process, any legislation proposed by the Government which involves the processing of personal data passes through the diligent filters of our office which ensures that the legal instrument contains the appropriate and specific provisions to adapt the application of the rules and principles contained in the Regulation.

The subject of artificial intelligence was placed front and centre during this year, due the new responsibilities which this office will assume under the Artificial Intelligence Act.

On 3 November, together with other national authorities and bodies, the Information and Data Protection Commissioner has been identified by the Government as a Fundamental Rights Authority for the purposes of article 77 of the AI Act – this role applies insofar as the processing of personal data is concerned. It is also expected that our office will be also designated as a market surveillance authority for certain high-risk AI systems as identified under Annex III of the AI Act.

02

Foreword

> **We will continue to support organisations in meeting their obligations, while placing the interests of individuals at the heart of everything we do.**

Whereas we recognised that society will benefit from AI technologies, it is essential to ensure that new technological developments are introduced in a manner that are fair, ethical, transparent and protect the fundamental rights of individuals, especially children and vulnerable persons.

In order to bring greater clarity to the application of data protection requirements in AI model training and deployment, and to reach a harmonised EU position and level playing field for industry, our Irish colleagues have requested a consistency opinion - pursuant to article 64(2) of the GDPR - from the European Data Protection Board on AI model development. The Board issued the opinion in December and this provided a unified position of three main issues, namely, the anonymity of AI models, the use of legitimate interest as a lawful basis to justify the processing of personal data, and the impact of unlawful processing in training AI model on the subsequent use of such model or system by the same controller or a separate one.

Looking ahead, we remain steadfast in our commitment to a rights-based approach – one that ensures emerging technologies are developed and deployed in ways that are fair, transparent, and lawful.

We will continue to support organisations in meeting their obligations, while placing the interests of individuals at the heart of everything we do.

The GDPR is working well and is standing the test of time. This clearly emerges from the report issued by the European Commission on the evaluation and review of the Regulation. The Commission examined in particular the application and functioning of Chapter V relating to the transfer of personal data to third countries or international organisations and Chapter VII on the cooperation and consistency mechanism.

During 2024, we have also closely monitored the developments regarding the Procedural Regulation under the GDPR, formally known as the Regulation on additional procedural rules for the enforcement of the GDPR. This regulation aims to harmonise and streamline how cross-border data protection cases are handled within the EU. It sets out clearer rules for cooperation between national data protection authorities, particularly in the one-stop-shop mechanism, introduces timelines, transparency measures, and rights for parties under investigation, including access to documents and the right to be heard. The goal is to ensure more efficient, predictable, and fair enforcement of the GDPR across the EU.

I would like to wholeheartedly thank my team for their expertise, dedication, and professionalism throughout the year. Together, we will continue to build a data protection framework that is resilient, adaptive, and always anchored in fundamental rights.

Ian Deguara
Commissioner

03

Mission, Vision and Strategic Objectives

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.

> **"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."**

During 2024, 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 on 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 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.

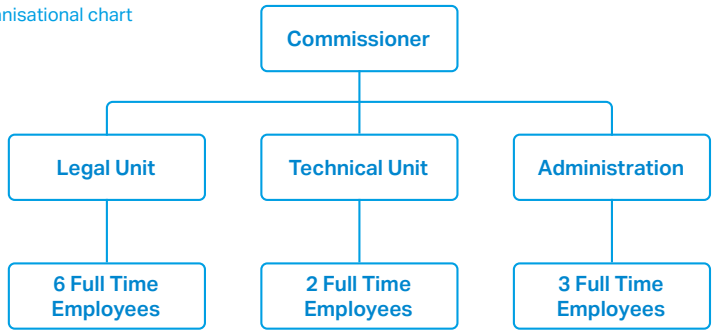
04

Organisation

04 Organisation

4.1 Organigram and Staff Complement

IDPC Organisational chart
2024



During the year under review, this office recruited three new employees, an officer responsible for human resources and office administration, and two lawyers who joined the legal team. Two employees, who provided long service to this office, retired. The Commissioner is committed to strengthen the staff compliment during 2025 by creating two new functions, namely a communications role and an international and European affairs one. The importance of giving visibility to this office's regulatory work is growing steadily and therefore the communications officer will be responsible to develop an effective plan designed primarily to get the message to the relevant audience by making use of the right communication channels. The role of an international and European affairs officer is indeed equally important in the light of the various commitments which this office has on a European level within the structures of the European Data Protection Board (EDPB).

4.2 Financial Resources

The financial resources which were allocated to this office, as a line item under the budgetary allocation of the Ministry for Justice during 2024, were €750,000. This marks a €50,000 increase over the subvention allocated in the previous year. Although this increase is not significant, the Commissioner is confident that the Government fully understands the important role of this office, and therefore providing adequate financial support will enable him to exercise his tasks and duties effectively and ensure that the fundamental rights of individuals with regard to the protection of their personal data are indeed safeguarded.

05

Summary of Data Protection Activities

05

Summary of Data Protection Activities

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 (SA) and is a key action of the same EDPB under its 2024-2027 strategy. It provides a structure for coordinating recurring annual activities by SAs which focus on a pre-defined topic and allows them to pursue this 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."

In 2024, the chosen topic for the third coordinated enforcement action was the "Implementation of the Right of Access", focusing on the EDPB Guidelines 01/2022 on the right of access and whether these guidelines are followed in practice. This topic is at the heart of data protection, one of the most frequently exercised data protection rights and one which SAs receive many complaints about. SAs including the IDPC used this exercise as a gauge to determine how organisations comply with the right of access in practice.

The main findings which emerged during the local investigation carried out by this office were very encouraging and showed that organisations have seriously considered and implemented their obligations in relation to the right of access as exercised by data subjects. The full CEF report as published by the EDPB lists inter alia, the issues and challenges that were observed by some controllers and provides a series of non-binding recommendations to help controllers in general implement the right of access. Despite these issues and challenges however, the EDPB acknowledged the fact that positive findings were observed across Europe.

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 2024, this office actively engaged with European and international counterparts to strengthen cooperation, promote consistency in enforcement and remain aligned with global developments in the field of data protection.

32nd European Conference of Data Protection Authorities (Spring Conference), Riga – Latvia, 14 to 16 May 2024

This office participated in the 32nd European Conference of Data Protection Authorities (Spring Conference), held from 14 to 16 May 2024 in Riga, Latvia. Organised by the Latvian Data State Inspectorate, this annual gathering brought together national supervisory authorities to discuss current challenges and collaborative approaches within the European data protection landscape. The agenda included discussions on the evolving role of data protection authorities amidst new digital regulations, safeguarding privacy in emerging technologies and balancing Anti-Money Laundering (AML) obligations with GDPR compliance. Sessions also focused on cross-border cooperation and health data governance in the digital age.

Privacy Symposium, Venice – Italy, 10 to 14 June 2024

In June 2024, this office attended the Privacy Symposium in Venice, Italy, hosted at the University Ca' Foscari from 10 to 14 June. This event served as a platform for over 300 experts and authorities to engage in interdisciplinary dialogue on global privacy challenges, regulatory developments and innovation in data governance.

Key topics included convergence of international data protection frameworks, compliance in light of rapid technological change and the future of research in privacy-enhancing solutions. The Commissioner also contributed as a panel speaker during the session entitled "Towards an Innovative Data Ecosystem in the Age of Artificial Intelligence – My Data is Mine 2024", which explored the implications of AI for data protection and fairness, particularly the use of synthetic data and public data scraping.

British, Irish and Islands' Data Protection Authorities (BIIDPA) Meeting, Larnaca - Cyprus, 26 to 27 September 2024

This office also took part in the British, Irish and Islands Data Protection Authorities (BIIDPA) meeting, held in Larnaca, Cyprus, on 26 and 27 September 2024. Hosted by the Cypriot Commissioner for Personal Data Protection, the meeting provided a forum for supervisory authorities to discuss shared enforcement challenges, exchange case-handling experience and explore regulatory developments within their respective jurisdictions.

46th Global Privacy Assembly, Jersey, 28 October to 1 November 2024

From 28 October to 1 November 2024, this office participated in the 46th Global Privacy Assembly (GPA), which took place in Jersey under the theme "The Power of I". The open sessions explored the intersection of innovation, integrity and individual rights in the digital age, with discussions addressing data protection in humanitarian contexts, the regulation of data flows, mental health implications and the role of supervisory authorities in a globalised information ecosystem.

5.2 EU and International Engagements

46th Global Privacy Assembly, Jersey, 28 October to 1 November 2024

During the closed sessions, several resolutions were adopted, including on the use of certification mechanisms, surveillance technologies, cross-border data transfers and the processing of personal data in neuroscience. These resolutions reinforced the commitment to enhancing transparency, accountability and global standards in data governance.

European Case Handling Workshop ECHW 2024, Tallinn - Estonia, 5 to 6 December 2024

Finally, this office contributed to the European Case Handling Workshop (ECHW), hosted by the Estonian Data Protection Inspectorate in Tallinn from 5 to 6 December 2024. This workshop provided a platform for data protection authorities to exchange operational insights from casework, particularly in relation to enforcement challenges, video surveillance, social media, IT security and controller-processor responsibilities. Discussions focused on practical resolution strategies and lessons learned from complex investigations, with the objective of fostering convergence in enforcement practices across the EU.

5.3 Participation in AI Workshop Organised by COE

This office was invited to attend the International Conference on "Artificial Intelligence and Data Protection: complementarity and an integrated approach" organised at the Council of Europe Headquarters, in Strasbourg, France, on 29 November 2024, under the auspices of the Secretariats of the Committee on Artificial Intelligence (CAI) and the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD) in collaboration with Strasbourg University (Centre for Fundamental Rights and Private Law). The conference brought together a number of experts and professionals from the invited supervisory authorities of the various member states to discuss the growing concerns of the use of artificial intelligence technology, in respect to the protection of personal data of data subjects.
The conference gave data protection authorities enhanced insight into the workings of generative AI models, such as large language models (LLMs), which are currently in the limelight from a data protection perspective. The sessions assisted competent authorities in their application of data protection regulations in the context processing undertaken by generative AI models, notably in the training, development and deployment stages. The sessions highlighted the vector-based nature of LLMs, and the novel manner in which data connections are made between one another in the virtual space and consequently the scope of processing undertaken between data sets which may include personal data, in order to obtain the requested output.

5.4 European Blockchain Sandbox

The European Blockchain Sandbox (EBS) is a regulatory sandbox initiative of the European Commission which offers entities such as start-ups, which intend to utilise Distributed Ledger Technologies (DLT), the opportunity to share their intended business proposition and their regulatory uncertainties. This is done in a confidential way with participating entities such as authorities, according to the legal domain/s concerned, for the opportunity that such provide legal advice and regulatory guidance on the uncertainties raised.

Following the success of the EBS first cohort, a second cohort was carried out, which gave supervisory authorities such as Malta's, the opportunity to gain insight on the issues being encountered in the area of DLT and data protection compliance. This office was involved in two use-cases operating in the Education and Banking and transaction due diligence areas, giving this office a unique opportunity to understand the industry practices being proposed or enquired under two main pillars of society.

The sandbox involved the review of each use-case over a number of meetings, every few weeks. This gave the participants and stakeholders the opportunity to assess the main subject matter, giving time to not only analyse the primary topics, but also developing notions. This additionally gave time for regulators to analyse and revert with any preliminary observations, as well as facilitated time for follow-up enquiries with the use-case owner. This ultimately enabled participants to better frame the main notions at play, and clarify the guidance required.

In the process, this office has reviewed the two use-cases, concerning novel solutions in the areas of Education and Banking via DLTs, and provided detailed and informative legal feedback of the data protection compliance aspects, following a review of the various data flows and topography of processing purposes amongst the various use-case stakeholders, as controllers and, or processors identified in the course of the assessment.

The IDPC acknowledges that DLT remains a challenging area in some cases, in terms of GDPR compliance, notably owing to its immutability, amongst other aspects. This office notes, in the course of providing its feedback to use-case participants, that native solutions from a DLT point of view are being found by some controllers in the DLT ecosystems, to address compliance for certain data protection aspects.

This office is of the opinion that the EBS regulatory sandbox has been beneficial for developing business offerings on both sides. From the regulatory side, it has provided unparalleled insight to supervisory authorities as to the possible measures which may be employed for achieving GDPR compliance, in instances which have remained principally challenging, whilst facilitating an ideal opportunity to guide institutions of the future in ensuring the fundamental rights of data protection of all EU data subjects concerned, in an controlled and confidential environment, which would otherwise, on account of resource and organisational issues, not ordinarily be sustainable.

5.4 European Blockchain Sandbox

Tying in with the success of the EBS, guidelines by the EDPB in relation to key data protection measures within DLTs have been forwarded to plenary for review and approval following joint liaison by supervisory authorities at expert subgroup ('ESG') level, after a hiatus, likely resulting from the emergence of the novel SARS-CoV-2 in early 2020. The SAESG plenary, which is expected to review the DLT guidelines between second and third quarter of this year, is anticipated to shed light on the data protection position for aspects which have not always been clear or certain, in the domain of DLTs.

Following the closure of the second cohort, this office has once again been invited for a further round of EBS regulatory sandbox participation, for which this office will once again provide data protection regulatory feedback to other participations during the EBS third cohort.

5.5 Local engagements

The past year has been a year packed with participation by this office in the public forum across a variety of industries and areas. On 3 December 2024, this office hosted a well-received session for educators, centred on the newly enacted AI Act and the applicable Data Protection Law, with a focus on key compliance considerations under the GDPR. The session was organized in partnership with the Ministry for Education, Sport, Youth, Research, and Innovation (MEYR) and brought together a diverse group of education officers, senior management, and other key stakeholders working on the new Digital Education Strategy.

This event was a key component of the IDPC's outreach program, aimed at empowering educators with practical insights into the legal and operational aspects of using AI in education. Attendees left the session with a much deeper understanding of the implications of the AI Act and GDPR in the context of digital education, better equipping them to confidently integrate AI technologies in ways that are both compliant and ethical.

The presentation highlighted the crucial connection between data protection and AI regulation, reinforcing how data protection law has already been safeguarding personal data and automated decision-making through the GDPR for over seven years, since its introduction. The attendees were able to appreciate how this legal framework directly impacts their use of AI tools in educational settings, such as when adopting AI for grading, assessment, or student support.

Rather than presenting data protection as a hurdle, the session framed it as an opportunity for educators to enhance their digital practices. The discussion emphasized that by adhering to GDPR requirements, educational institutions could foster trust with students, parents, and the wider community, ensuring that AI is used responsibly and transparently.

5.5 Local engagements

Educators gained practical insight as to implementing AI in ways which protect students' rights while boosting their teaching effectiveness and efficiency.

One of the key takeaways was the practical pointers on how to avoid potential risks that AI software could pose to students' fundamental rights. By equipping educators with this knowledge, the session helped to mitigate concerns around privacy, bias, and fairness in automated decision-making. Educators were given clear guidelines on how to manage student data responsibly, ensuring that AI tools are used in a way which benefits both educators and students alike.

The session additionally offered tangible solutions for addressing potential challenges, such as the use of AI in personalized learning or automated grading. Educators walked away with comparable use-case examples to ensure that students' data protection rights are upheld, all while maximizing the positive impact AI can have on their educational journey. This included understanding how to maintain transparency and fairness when using AI and how to ensure that automated systems are used in a manner that enhances learning outcomes without compromising students' privacy - an encapsulation of the human in the loop, an underlying driving principle introduced under the GDPR with the right not to be subject to automated decision-making.

The positive reception from attendees reflected the success of the event. Many expressed appreciation for the opportunity to engage in a collaborative discussion, share concerns, and exchange thoughts in respect to the ethical and compliant use AI in the classroom. Towards the end of the session, it become clearer how the session fostered a stronger sense of confidence among educators in navigating the evolving landscape of data protection and innovative tools such as AI, by synthesising the main notions and likely areas of applicability, reinforcing the commitment to a safer, more ethical use of technology in education.

The presentation was made possible through a close collaboration with the Malta Digital Innovation Authority (MDIA) team, highlighting the importance of cross-sector partnerships in advancing digital education initiatives. Held at the Digital Literacy Centre in Ħamrun, the venue provided an ideal space for educators to strengthen their understanding of AI integration and data protection of students, prevalently minors, and hence a group of individuals recognised as being more vulnerable.

This session marked a significant step forward in preparing Malta's education sector for the digital future. By equipping educators with the principles and tools they need to navigate both AI and data protection law, this office continues to play a vital role in shaping a future where AI can be used to enhance learning while ensuring privacy and long-term fairness for all students.

05

Summary of Data Protection Activities

5.6 Engagement with Local Regulatory Authorities

In 2024, this office had several meetings with other national regulatory authorities, namely the Malta Communications Authority, the Malta Gaming Authority and the Malta Financial Services Authority. The Commissioner considers that ensuring coordination and cooperation with other authorities on cross-regulatory matter is indeed important. These meetings focused on aligning regulatory approaches, sharing best practices, and discussing overlapping areas of concern. Strengthening these relationships enhances regulatory consistency and helps ensure more effective oversight across sectors. This office remains committed to ongoing dialogue and joint initiatives with local stakeholders.

5.7 DISC Research Cluster – University of Malta

During the year under review, the Commissioner was invited to join the Executive Committee of the Data Integrity and Stewardship Cluster (DISC) at the University of Malta. DISC is a multidisciplinary research initiative focused on overcoming the legal, social, and technical challenges of data processing for scientific research while ensuring the protection of participant rights. The Cluster's research covers important areas such as biomedical imaging, genomics, and data protection, and it is supported by pillars that span across the fields of law, science, technology, and society.

The Executive Committee, which governs and manages the Cluster, is composed of experts from diverse fields, including both internal members from the University and external stakeholders. The Commissioner's participation on the committee was considered relevant in the light of his expertise in the field of the protection of personal data. During the first meetings, it was agreed that the main priority deliverable of the committee will be to develop a legal framework, under the Data Protection Act, to regulate data banks and scientific research in Malta. It is expected that the draft regulations will be developed and finalised before the second quarter of 2025. The process will involve engaging and consulting with the relevant stakeholders in the area.

05

Summary of Data Protection Activities

5.8 Participation in Radio Programme

As part of its outreach strategy, this office regularly participated in a live radio programme, with phone-ins, where various data protection topics were discussed. These topics were tailored to the audience of this programme, who are generally not data protection experts but listeners who are aware of their rights and feel comfortable to contribute by voicing their concerns on issues which affect their daily lives. The Commissioner takes the citizens' concerns seriously and there were few, but very specific, instances where callers were encouraged to provide this office with all the details related to the issue for an ex-officio investigation to be initiated.

5.9 Recognition of Ethics Committee

Article 7 of the Data Protection Act makes a 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 the Institute of Microbiome and Applied Sciences (IMAS) was formally recognised by the Commissioner, as the Ethics Committee for research carried out by IMAS.

This formal recognition was provided following consultation meetings with IMAS. As part of the request for such formal recognition, procedures and guidelines were developed by IMAS and duly considered by the Commissioner. Other documents such as the "Participant Information Sheet" and "Informed Consent Form", 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 the IMAS was recognised as a committee having the function to evaluate academic research projects or research projects supported by external funding agencies in terms of the aforementioned article 7. This recognition was given subject to a number of conditions which include:

- that the IMAS 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;
- that the Commissioner may request any clarifications or verifications;
- that recommendations for final approval are to be submitted to the Commissioner for his final approval.

5.10 Delivery of Data Protection Lectures - Employment course – MEA

In collaboration with the Malta Employers' Associations (MEA), this office once again delivered for another year, a series of informative lectures to members of the MEA, keeping with its commitment of proactively raising awareness and educating the public and industries on the subject and application of EU and domestic data protection law. The sessions comprised of Human Resources personnel and other employment-focussed professionals, concentrating on the practical application of the GDPR within the context of employment. These sessions aimed to raise awareness among both employers and employees about their respective obligations and responsibilities in the workplace, under EU and domestic data protection law.

Key topics which were discussed included the principles of the GDPR as they may find application in an employment context as well as specifically, the lawfulness of processing employee personal data, particularly the limitations of relying solely on consent in the employer-employee relationship due to inherent power imbalances. This office reiterated the importance of relying on more appropriate legal grounds such as contract performance (and necessity), or a legal obligation, where relevant, while ensuring the principles of necessity and proportionality are also respected where employee personal data is processed in accordance with such legal basis.

The lectures also covered transparency obligations, highlighting the requirement for employers to clearly inform staff about how their personal data is collected, used, and retained through the appropriate privacy and data protection policies. Particularly, employee surveillance was also discussed to ensure any such monitoring which may be utilised by employers is not intrusive or otherwise in violation of the GDPR's principles. Special attention was given to sensitive categories of data, such as health and medical related or disciplinary records, which require additional legal considerations and safeguards at and record keeping and administration levels.

Further discussion focused on data retention practices concerning employee personal data, on the basis of the data minimisation and storage limitation principles in relation to separate statutory obligations prescribing the retention of certain information and records which may include employee personal data.

Overall, the sessions endeavoured to provide valuable clarification and practical guidance, helping members of the MEA navigate GDPR requirements more confidently while safeguarding the rights of their personnel.

06

Data Protection Regulatory Work

06

Data Protection Regulatory Work

6.1 Contacts and Enquiries

Throughout 2024, a substantial number of individuals and entities have reached out to this office and enquired for its expertise to clarify data protection-related aspects.

Enquiries were received in relation to the use of generative AI within the context of education and learning - these indicate that educational institutions are becoming increasingly aware of the importance of their position as educators in respect of the rights and freedoms of students within the context of the GDPR and the long-term effects which infringements of this rights and safeguards may have on individuals.

School personnel have enquired for instance in terms of the potential risks of generative AI use such as the current ChatGPT in terms of data storage, which may include personal data, for AI model training purposes, as well as safeguards which may be employed to mitigate risks, by educators, to the extent possible.

This office has been contacted to provide guidance on safety monitoring of publicly accessible spaces of risk, such as public beaches, through the use of surveillance and AI technologies.

The proposed processing would be intended to assist lifeguards in identifying individuals who may be encountering swimming difficulties. Given that lifeguards' role includes constant monitoring of the whole beach with numerous individuals entering and exiting the water constantly, and the wide scope of perimeter to monitor, such technically would assist lifeguards identify immediately a swimmer in difficulty, possibly saving seconds, which may be crucial in such critical circumstances.

Feedback was provided in relation to this proposed measure, after careful and holistic assessment of the numerous aspects involved in the processing, whilst also guiding the enquirer with best data protection practices in order to mitigate possible risks, owing to the extensive, indiscriminate and type of data being recorded of individuals whilst on the beach.

A number of enquiries have been received by this office, over all contact channels, as to the permissibility and legality considerations of installing and operating CCTV surveillance or their legality and rights when these are already affixed, within a block which hosts a number of residents and hence falls within the regime of the Condominium Act, Chapter 398 of the Laws of Malta.

The Commissioner also received enquiries on and guided gaming companies in order to comply with data subject access requests in the context of gaming customers. Apart from reiterating the legal position on the extent to which a restriction may be involved pursuant to the subject access request invoked, this office also guided gaming operators on the corresponding obligations prescribed on them as a result of a data subject access request made by one of their customers, how to completely fulfil such requests, and specifics on deadline extensions, amongst other pertinent considerations.

06

Data Protection Regulatory Work

6.2
Advisory Services

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

In 2024, the Commissioner was requested to provide advice to the Government on several legislative measures concerning the protection of the rights and freedoms of natural persons in relation to the processing of personal data. This advisory role is carried out in accordance with article 36(4) of the GDPR, which requires that the Commissioner shall be consulted during the preparation of legislative proposals that involve personal data processing.

> **The Coordinated Vulnerability Disclosure Policy is primarily intended to support responsible organisations in the implementation of such policy with a view to encourage the ongoing testing of its ICT systems.**

During the reporting year, the Commissioner was formally consulted on the following legislative instruments:

- Local Enforcement System Agency Establishment Order, Subsidiary Legislation 595.14;
- Gender-Based Violence and Domestic Violence Act, Chapter 581 of the Laws of Malta;
- Aġenzija Sapport (Establishment as an Agency) Order, Subsidiary Legislation 595.18;
- Health Act (Cap. 528 of the Laws of Malta);
- Schengen Information System Regulations, Subsidiary Legislation 164.04;
- Gender Identity, Gender Expression and Sex Characteristics Act, Chapter 540 of the Laws of Malta; and
- Food Safety and Security Authority Bill.

6.2.2 Advice provided to Public Authorities

Malta Digital Innovation Authority – Coordinated Vulnerability Disclosure Policy

The Malta Digital Innovation Authority consulted the Commissioner in relation to the drafting of the Coordinated Vulnerability Disclosure Policy, which is a formalised set of rules for searching and reporting vulnerabilities, with an emphasis on coordinated disclosing information about these vulnerabilities.

The Coordinated Vulnerability Disclosure Policy is primarily intended to support responsible organisations in the implementation of such policy with a view to encourage the ongoing testing of its ICT systems, allowing for vulnerabilities to be identified and addressed, which ultimately improves the security of the ICT systems.

The Commissioner was consulted in relation to issues pertaining to the protection of personal data which may arise in case the security researcher detects a vulnerability threat that may lead to any form of processing within the meaning of article 4(2) of Regulation (EU) 2016/679.

06

Data Protection Regulatory Work

6.2 Advisory Services

6.2.2 Advice provided to Public Authorities

Data Protection and Information Coordination Unit – Data Protection Policy

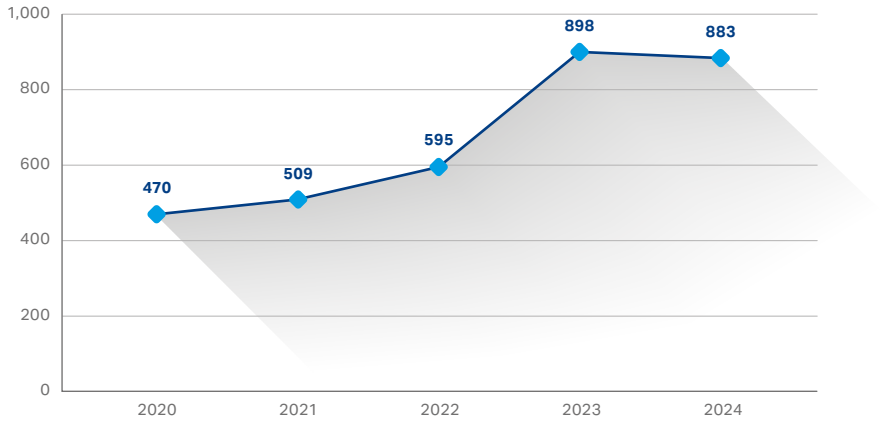
In the case of 'Rebecca Bonello vs National School Support Services', the Court of Appeal found that the data protection policy of the controller failed to meet the minimum informational requirements set out in articles 13 and 14 of Regulation (EU) 2016/679. As a result, the Data Protection and Information Coordination Unit within the Ministry for Justice and the Reform of the Construction Sector initiated a revision of the templates used by public authorities. The Commissioner was actively consulted throughout this process to ensure full compliance with the principle of transparency and the related informational obligations under the Regulation (EU) 2016/679.

6.3 Complaints

6.3.1 Data Protection Complaints

In 2024, this office received a total of eight hundred eighty-three (883) local complaints. Although slightly lower than the 898 complaints recorded in 2023, the figure remains significantly higher than in earlier years, illustrating a consistent rise in individuals seeking redress under data protection law. For comparison purposes, this office received eight hundred ninety-eight (898) complaints in 2023, five hundred ninety-five (595) in 2022, five hundred nine (509) in 2021 and four hundred seventy (470) in 2020, meaning that the total number of complaints has nearly doubled over the past five years. Despite a marginal decline from 2023, the 2024 total still constitutes an 88% increase compared to 2020.

Complaint comparison by year



06

Data Protection Regulatory Work

6.3 Complaints

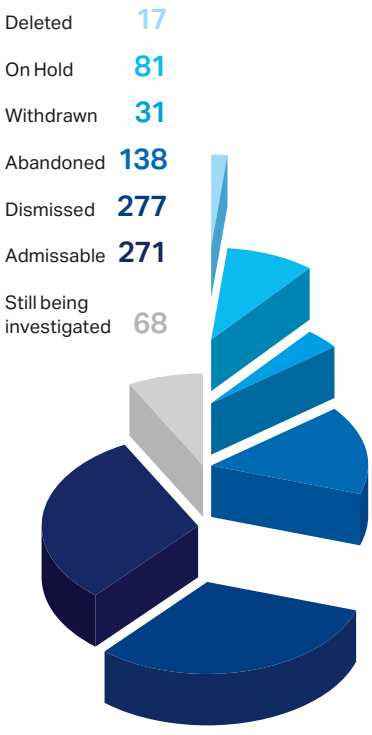
6.3.1 Data Protection Complaints

These complaints were processed through a structured case-handling system, resulting in a variety of outcomes. By year-end, the breakdown was as follows: seventeen (17) complaints were deleted, eighty-one (81) were placed on hold, thirty-one (31) were formally withdrawn, one hundred thirty-eight (138) were abandoned, two hundred seventy-seven (277) were dismissed, two hundred seventy-one (271) were found to be admissible and sixty-eight (68) remained under active investigation.

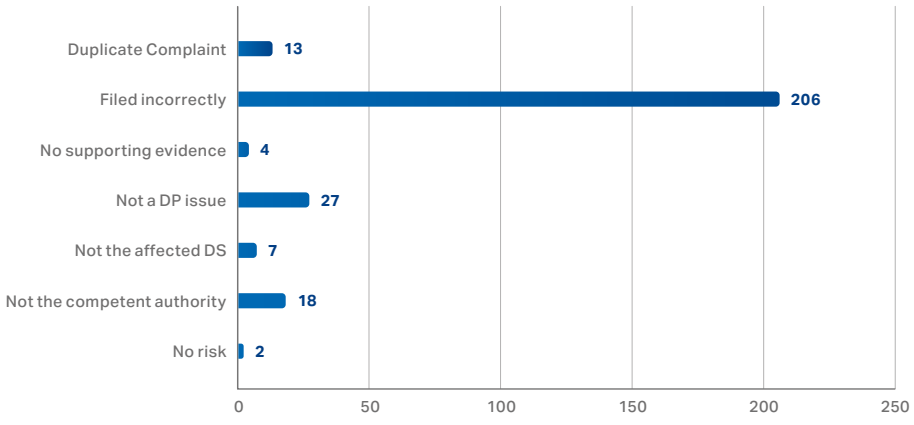
A total of seventeen (17) complaints were deleted during the year. Complaints are typically deleted when they are identified as spam, are administratively duplicated or have been submitted in an incomplete format. Eighty-one (81) complaints were placed on hold, usually because they concern the same subject matter and legal interpretation previously addressed by the Commissioner. During 2024, the Commissioner issued several decisions involving such interpretations. In view of the number of identical cases that had already been investigated, where the controller is now contesting the legally binding decision before the Information and Data Protection Appeals Tribunal, the Commissioner has decided to temporarily place related complaints on hold until the Tribunal delivers its judgment. This approach ensures that consistent and fair rulings are applied to all cases involving the same subject matter. Once the matter becomes res judicata, this office will resume each affected case and proceed with the investigation accordingly.

A further one hundred thirty-eight (138) complaints were classified as abandoned. This typically occurs when complainants fail to respond to follow-up requests or stop communication, often owing to a failure to submit essential supporting documentation such as authorisations or the necessary translated materials. During the year, thirty-one (31) complaints were formally withdrawn by the data subjects themselves, normally when the complainant opt not to proceed with the matter.

Complaints received during 2024



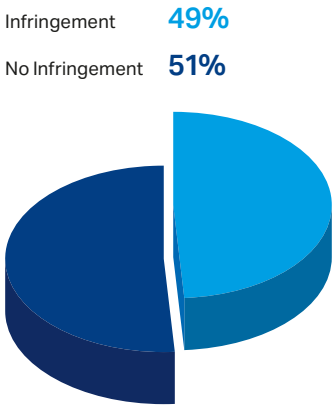
Cases formally dismissed



06

Data Protection Regulatory Work

6.3 Complaints

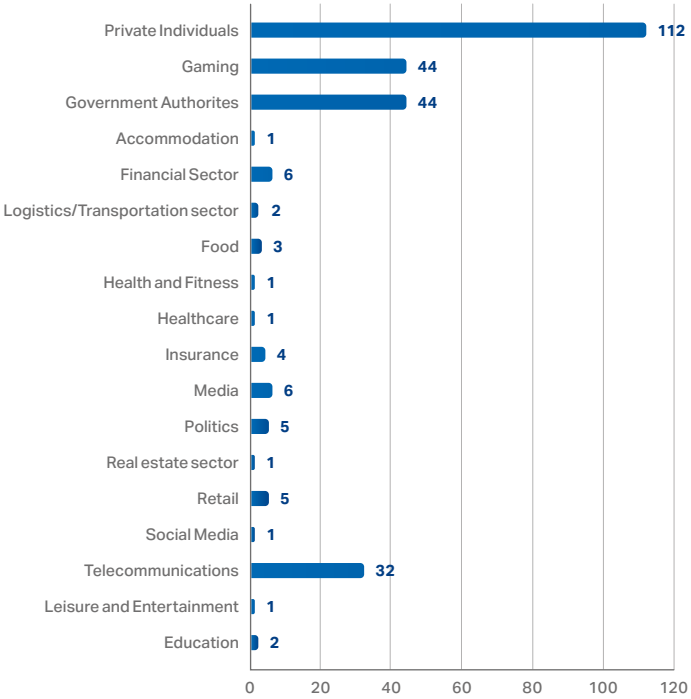


6.3.1 Data Protection Complaints

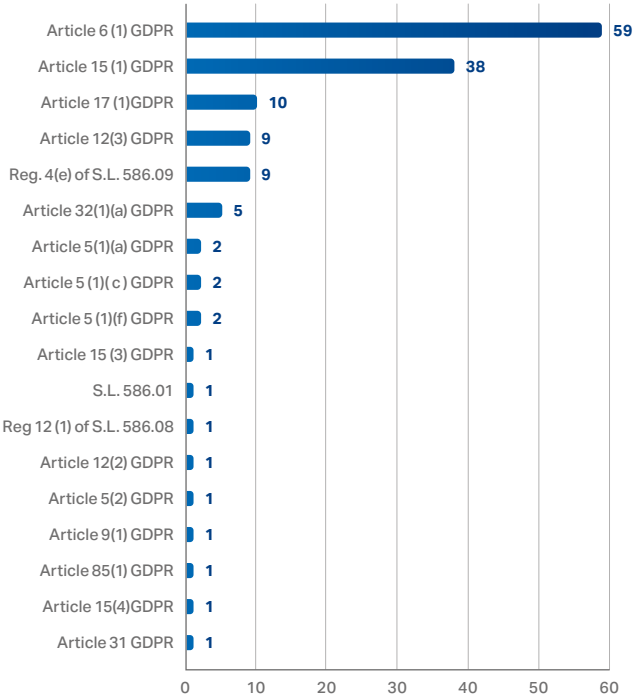
A total of two hundred seventy-seven (277) complaints were formally dismissed following initial assessment. These complaints are dismissed due to procedural deficiencies, such as failure to submit adequate documentation or concern a data protection issue. The most common ground for dismissal during the reporting year was incorrect filing, which accounted for two hundred six (206) cases. Other reasons included the complaint falling outside the Commissioner's competence, the subject matter not being related to data protection or duplication of previously submitted complaints.

Out of the total complaints received, two hundred seventy-one (271) were found to be admissible, having satisfied all legal requirements for investigation. The admissible complaints spanned several sectors, with one hundred twelve (112) originating from private individuals, forty-four (44) from the gaming industry, forty-four (44) from government entities and seventy-one (71) from other sectors, among which the telecommunications sector featured most prominently with thirty-two (32) cases.

Admissible cases by Sector



Article Infringements

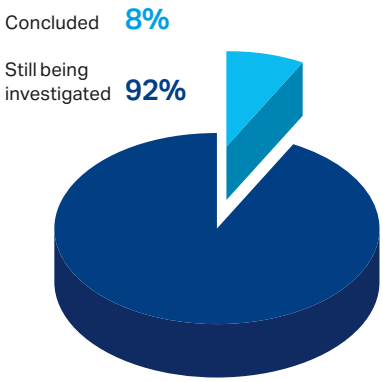


06

Data Protection Regulatory Work

6.3 Complaints

Cases not concluded in 2024



6.3.1 Data Protection Complaints

In total, two hundred forty-five (245) admissible cases were investigated and concluded within the year. From these concluded investigations, one hundred twenty-one (121) resulted in findings of infringement, while one hundred twenty-four (124) were determined not to involve any breach of data protection law. For non-infringement outcomes, two (2) were resolved amicably and one hundred twenty-two (122) were closed with a determination of no infringement. In cases where an infringement was found, one hundred and nineteen (119) culminated in decisions issued by the Commissioner and two (2) were resolved through amicable settlements. The infringements identified across the one hundred twenty-one (121) cases touched on several key provisions of the GDPR and national legislation. The most frequently breached article was article 6(1) GDPR, the lawful basis for processing, which was infringed in fifty-nine (59) cases. Article 15(1) GDPR which relates to the right of access was breached in thirty-eight (38) cases and article 17(1) GDPR, relating to the right to erasure, in ten (10). Several decisions cited multiple infringed provisions.

In response to these investigations, the Commissioner issued several orders in 2024, particular emphasis was placed on failures to respond to subject access requests, especially within the gaming sector, where controllers repeatedly failed to respond within the legally required timeframe. In such cases, the Commissioner required controllers to provide documentation proving that the SAR had been fulfilled, to demonstrate that access had been granted or where no evidence was submitted, issued an order via a formal letter ordering the controller to respond immediately. Improper deployment of CCTV systems was also a recurring theme. In several cases, CCTV cameras were found to be positioned in a manner that monitored public areas or neighbouring private property, breaching the principle of data minimisation. The Commissioner ordered that these CCTV cameras be reconfigured to ensure that monitoring was strictly limited to the property owned by the controller.

In the telecommunications sector, this office received multiple complaints from individuals who had received postal correspondence clearly intended for unrelated third parties. Upon investigation, these incidents were traced to flawed address-linking mechanisms in provider databases. The Commissioner determined that such systemic errors constituted a violation of the GDPR's accuracy principle. Consequently, these service providers were ordered to update their internal procedures, adopt more rigorous data verification mechanisms and erase any inaccurately held personal data arising from these breaches.

By the end of the reporting year, sixty-eight (68) complaints remained under active investigation. In these cases, the investigation was not concluded within the same calendar year and therefore remained ongoing.

> **"In the telecommunications sector, this office received multiple complaints from individuals who had received postal correspondence clearly intended for unrelated third parties. Upon investigation, these incidents were traced to flawed address-linking mechanisms in provider databases."**

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 Information and Data Protection Commissioner in 2024. 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.

Data Subject Access Requests & Data Protection Shortcomings

On 4 May 2023, the Commissioner issued a decision following a complaint alleging that the controller, which provided speech and occupational therapy services at the complainant's son's school, had acted in a manner that infringed the provisions of the Regulation. Although the Information and Data Protection Appeals Tribunal had overturned the decision of the Commissioner, the Commissioner appealed the Tribunal's decision. Consequently, the Court of Appeal upheld the Commissioner's decision in its entirety, deciding against the controller.

> **"The complainant sought to exercise her right of access under article 15 of the Regulation to obtain a copy of her minor son's personal file from the controller – specifically, all his records relating to these therapy services."**

As to the facts of the case, the controller provided speech and occupational therapy services at the complainant's son's school, which intended to support young children's development. As part of these services, therapists conducted individual assessments and recorded their observations in each child's personal file. The complainant sought to exercise her right of access under article 15 of the Regulation to obtain a copy of her minor son's personal file from the controller – specifically, all his records relating to these therapy services. However, she complained that the process was far from straightforward, and that this highlighted several data protection shortcomings on the controller's part.

Principally, the complainant alleged that the controller failed to acknowledge and fulfil her access request in a timely manner, and never provided a justification for its delay. Additionally, the complainant alleged that the controller had not made its data protection policy easily accessible on its website, and that it failed to include the minimum information to be given to data subjects in the policy, nor did it provide clear information about the controller's identity – making it difficult to direct access requests and other data subject requests to the correct channels. The controller had tried to argue that the complainant failed to specify the content of her access request and had not directed it to its data protection officer, and that this is what caused the delay.

6.3 Complaints

6.3.2 Summaries of Key Data Protection Cases

Data Subject Access Requests & Data Protection Shortcomings

The controller also explained that even though it did not send a copy of the personal data to the complainant as she had requested, it had invited the complainant to view her son's file in-person.

In the decision, it was highlighted that controllers must facilitate, and not further complicate, the exercise of data subject rights under the Regulation.

"The controller also explained that even though it did not send a copy of the personal data to the complainant as she had requested, it had invited the complainant to view her son's file in-person."

When analysing the manner in which the complainant attempted to exercise the right of access, the Commissioner referred to the EDPB Guidelines 01/2022, which provide that even if the data subject makes his/her request to the controller's general email and not directly to its DPO, the controller must make all reasonable efforts to handle the request, so that it can be redirected to the correct contact point and answered within the time limits imposed by the Regulation. In the legal analysis of the case, it was also emphasised that the purpose of an access request is to enhance transparency vis-a-vis data subjects and strengthen their control over their personal data.

In addition, the Commissioner's legal analysis examined the position of children as vulnerable natural persons - recital 38 of the Regulation provide that "children merit specific protection with regard to their personal data" and recital 75 classifies children as "vulnerable natural persons". In this case, the Commissioner considered that the controller had the role of providing services to children, young people, and their parents. Consequently, the children's data, particularly their health data, required enhanced protection. Finally, the case also highlighted the importance of ongoing data protection training for staff involved in processing. Staff must be able to recognise when an access request has been made, as this helps to prevent issues from arising at later stages, such as delayed responses and non-compliance with the Regulation.

In the Commissioner's decision, the controller was found to have infringed a number of provisions of the Regulation, namely; failing to fulfil the complainant's access request within the timeframe of one month, not providing the requested information to the complainant under article 15 of the Regulation, failing to properly involve its data protection officer in the case, acting in breach of the principle of transparency – including because its data protection policy lacked even the minimum information required under articles 13 and 14 of the Regulation, and not having an internal data protection notice for its employees. Consequently, the Commissioner had decided that the imposition of an administrative fine of €2,500 to be paid by the controller was both necessary and appropriate given the nature and gravity of the infringement.

6.3 Complaints

6.3.2 Summaries of Key Data Protection Cases

Unsolicited Direct Marketing

On 28 June 2024, the Commissioner issued a decision following a complaint alleging that unsolicited marketing calls were being made to the complainant's mobile numbers, despite having been assured by the controller (in the context of a previous complaint) that her personal data had been erased and her mobile numbers barred from the controller's systems. The complainant alleged that following her first complaint, which was lodged in 2022, she continued to receive frequent phone calls and SMSs advertising the products and services offered by the controller.

"The complainant alleged that following her first complaint, which was lodged in 2022, she continued to receive frequent phone calls and SMSs advertising the products and services offered by the controller."

The controller rebutted the allegations, arguing that following the first complaint it had promptly erased the complainant's personal data, and that the recent phone calls were erroneously made because of a software used by the controller to randomly generate numbers to be contacted for marketing purposes. Because the numbers were generated at random by the software, the controller argued that the identity of the call recipients was unknown, and therefore there was no processing of personal data. Nevertheless, it acknowledged the incident and stated that it had introduced new preventative measures, including adding a barred list of numbers to the controller's centralised telephone system.

The complainant, however, disputed the controller's arguments, stating that other emails sent by the controller referenced her full name, professional title, and both mobile numbers, indicating that her personal data was still being processed. Additionally, the complainant stated that even after explicitly requesting the deletion of both her mobile numbers via an email sent to the controller in May, she still received another phone call on her second number in June. The controller tried to defend its position, arguing inter alia that while the complainant's mobile numbers had been blocked from its internal systems after the first complaint, the recent calls were made by sub-contracted individuals using their personal phones, an error that the controller confirmed had since been addressed.

However, following this, the complainant informed this office that she once again received an unsolicited marketing call. When asked for its feedback on this, the controller explained that it had recently migrated to a new provider after terminating its sub-contracting agreement due to reliability concerns. The controller explained that a technical error had occurred during the migration – where previously blocked numbers were inadvertently unblocked.

6.3 Complaints

6.3.2 Summaries of Key Data Protection Cases

Unsolicited Direct Marketing

Following a lengthy and thorough investigation, the Commissioner concluded that despite the controller's repeated assurances, the complainant continued to receive unsolicited marketing. Consequently, the Commissioner decided that the controller had infringed article 21(2), as it failed to respect the complainant's right to object to processing for the purposes of direct marketing, and article 5(2) of the Regulation as the controller failed to demonstrate its compliance with the provisions of the Regulation as required by the principle of accountability.

"Following a lengthy and thorough investigation, the Commissioner concluded that despite the controller's repeated assurances, the complainant continued to receive unsolicited marketing."

In light of this, and after considering the persistence of the controller's infringements, the Commissioner decided that the imposition of a €15,000 administrative fine against the controller was necessary to respond to the nature and gravity of the infringement.

Secure Processing of Personal Data

On 2 February 2024, the Commissioner issued a decision following a complaint where the complainant alleged that the controller had misplaced her medical records. The complainant explained that she was asked to provide her health records, which had been generated elsewhere, to the controller prior to surgery. The usual procedure of the controller was to make copies of the original health records and immediately return them to the patient. However, in this particular case, the controller's staff forgot to return them, requiring the complainant to collect them on a later date.

Due to the complainant's limited mobility, the earliest she could collect the documents was in around a month. During this period, the documents were left at the controller's reception stored in an unlocked box file. When the complainant eventually came to collect the documents, she was informed they had been lost. The controller explained that they had been misplaced by the reception staff, who were not trained on how to safely store health records.

In the process of the investigation, the Commissioner considered that patient medical data is a special category of personal data under article 9 of the Regulation, meriting special protection. Bearing in mind, also, the obligation imposed on controllers under article 32 of the Regulation to implement technical and organizational measures to ensure secure processing, the Commissioner requested the controller to provide information about the procedures it has in place to securely handle personal data, including; its current procedure for the manual storage of patient health records, the security measures it implemented to ensure their secure processing, the access controls it had in place and the action taken, if any, to locate the complainant's lost health records.

6.3 Complaints

6.3.2 Summaries of Key Data Protection Cases

Secure Processing of Personal Data

The Commissioner's investigation revealed that the untrained reception staff failed to recognize the importance of securely storing personal data. In addition, the controller had employed some security measures (such as implementing access restrictions via RFID, using CCTV surveillance, and having a secure medical records room), and had begun revising its processes to ensure the more secure handling of personal data. However, crucially, it transpired that the controller had not treated the documents as sensitive medical data but as a belonging left behind by the complainant.

> **"The Commissioner determined that given the nature of the personal data involved (medical health records of patients) the risk associated with processing was very high."**

The Commissioner determined that given the nature of the personal data involved (medical health records of patients) the risk associated with processing was very high. In this case, the Commissioner determined that the controller had failed to implement the appropriate security measures to address this risk, and that this compromised the confidentiality and availability of the personal data involved, ultimately resulting in an infringement of article 32(1)(b) of the Regulation.

This case underscored the importance for controllers to implement and enforce technical and organizational measures appropriate to the risks involved. Controllers should have robust policies and procedures in place for securely handling and storing personal data, including contingency procedures, and should prioritise ongoing employee training to ensure patient confidentiality. The case also highlighted how controllers must have a clear understanding of when they are processing personal data, given that the definition of 'processing' under the Regulation is wide, including the collection and storage of personal data – even where that personal data has not been generated directly by the controller.

Information Obligations of Controllers

On 2 February 2024, the Commissioner issued a decision following a complaint concerning the processing of personal data via hand-hand speed cameras. The complainant claimed that the Malta Police Force (the controller) had used hand-held speed cameras on public roads covertly, and consequently, breached the Regulation's principles of fairness and transparency. The complainant claimed that there were no signs placed in nor before entering the area where the cameras were being used, informing drivers that their personal data will be collected.

The controller tried to argue that providing this information to drivers was not necessary when hand-held speed cameras are used because – unlike fixed speed cameras which monitor the road continuously – hand-held cameras only collect driver personal data when an officer suspects a vehicle is over-speeding. Additionally, the controller argued that it had already fulfilled its information obligations vis-à-vis data subjects by publishing the relevant information about processing on its website.

6.3 Complaints

6.3.2 Summaries of Key Data Protection Cases

Information Obligations of Controllers

The complainant maintained that data subjects have a right to be well informed about the processing of their personal data, and that posting on its website was not sufficient to satisfy its information obligations as a controller.

The Commissioner's investigation involved an in-depth analysis of the provisions of the Regulation, of the Charter of Fundamental Rights of the European Union, judgements of the European Court of Justice, the EDPB Guidelines, as well as the local law regulating processing via high-speed cameras (Subsidiary Legislation 586.08 - the Processing of Personal Data by Competent Authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties Regulations).

> **"With regards to the personal data collected, the Commissioner's investigation revealed that high-speed cameras captured the vehicle's registration plate, speed, location, and time."**

With regards to the personal data collected, the Commissioner's investigation revealed that high-speed cameras captured the vehicle's registration plate, speed, location, and time. The Court of Justice of the European Union had previously ruled that, given that the definition of personal data includes "any information relating to an identified or identifiable individual", a vehicle information number (VIN) can be considered as personal data if the controller is able to associate it with a specific individual. In the case at hand, the controller did have the means to link the VIN with specific individuals.

With regards to the concept of 'processing' under the Regulation, the decision made it clear that the definition of 'processing' is not limited to specific devices and any device that can carry out a processing operation falls within the definition of 'processing'. Therefore, high-speed hand-held cameras were not excluded from its scope. Furthermore, both the Charter in article 8(2) and the Regulation in article 5(1)(a) recognise the principle of fairness when processing personal data, which requires that data subjects are informed in a meaningful way, and at the time the personal data is obtained, about the processing activity, its purposes, and who is collecting it.

In this case, the Commissioner decided that the controller had failed to satisfy its information obligations under the Regulation and the local law, and had acted in breach of the principle of fairness. Consequently, the controller was ordered to display the appropriate signs, within a reasonable distance, so that data subjects can be well informed of and easily understand the circumstances of the processing of their personal data.

This case highlights the importance of ensuring that the processing of personal data is always carried out in line with the principle of fairness, which underpins the entire data protection framework and which requires that controllers act fairly vis-à-vis data subjects, by providing them with clear information about how their personal data is processed.

6.4 *Ex-officio* Investigations

In 2024, the Commissioner initiated several ex-officio investigations as part of the ongoing efforts to monitor and enforce compliance with the GDPR, following indications of potential infringements in some sectors.

Cookie Banner Investigation

A significant area of focus was the examination of website cookie banners. Investigations were conducted on websites, with a particular emphasis on controllers in the financial sector, that were found to be missing cookie banners or not complying with all the requirements. Assessing the controllers' website allowed the Commissioner to immediately identify clear instances of non-compliance. All controllers subsequently cooperated fully and swiftly took steps to ensure compliance with the law.

> **"As a corrective measure, the controller implemented a new internal policy requiring that all system changes undergo prior review and approval by senior personnel."**

Password Management Investigation

The Commissioner initiated an ex-officio investigation regarding the handling of user passwords by an online sales website. The controller confirmed that, in late May 2024, a system glitch had resulted in a limited number of customers receiving emails containing unencrypted passwords. The issue was attributed to an oversight by a junior staff member during a system update.

As a corrective measure, the controller implemented a new internal policy requiring that all system changes undergo prior review and approval by senior personnel. The Commissioner acknowledged the controller's prompt and collaborative response, as well as the steps taken to strengthen internal controls and prevent future incidents.

AI Camera Investigation

A social media post concerning the installation of a camera with artificial intelligence (AI) functionalities in a locality in Malta prompted the Commissioner to initiate an ex officio investigation. The purpose of the inquiry was to obtain further information from the Local Council in order to assess the operational features of the camera and determine its compliance with the applicable regulatory requirements. Following the receipt of the requested information, the Commissioner carried out an on-site inspection to directly examine the camera's functionalities and capabilities. The investigation established that, although the camera is technically capable of utilising AI for activities such as facial recognition, the Commissioner verified that no such processing is being carried out.

6.4 *Ex-officio* Investigations

Investigation vis-à-vis the Electronic Communications Service Providers

In response to media reports that data subjects had received correspondence at their residential addresses intended for third parties, the Commissioner initiated an ex-officio investigation.

The purpose of the investigation was to evaluate whether the procedures implemented by the electronic communications service providers were in line with their obligations under the GDPR, with particular reference to the principle of accuracy as set out in article 5(1)(d). The investigation focused on assessing whether appropriate identity and address verification checks were being carried out during the customer onboarding process and at any subsequent stage involving the collection and processing of personal data for service delivery.

> **"As a result of the investigation, the Commissioner instructed two service providers to amend their internal procedures and to erase personal data that had erroneously linked the data subject's residential address to a third party."**

As a result of the investigation, the Commissioner instructed two service providers to amend their internal procedures and to erase personal data that had erroneously linked the data subject's residential address to a third party. Both controllers have since confirmed that the required corrective actions have been implemented.

Investigation into alleged unlawful processing of a special category of personal data

The Commissioner initiated an ex-officio investigation following information received concerning allegations that former employees of a controller had access to a database that contained information revealing political opinions. The scope of the ex-officio investigation was to determine whether the controller processed any personal data, including special categories of personal data, which led to an infringement of the provisions of the GDPR and the rights and freedoms of the data subjects.

In accordance with the investigative powers conferred by article 58(1) of the GDPR, the Commissioner engaged an external digital forensic auditor to assist in the technical aspects of the investigation. The auditor conducted a forensic analysis of the extracted data and submitted a report of findings to the Commissioner. The report concluded that the dataset "did not include any data sources which may be linked to the alleged leaked database reported". In light of the findings presented by the external auditor, the Commissioner did not identify any evidence indicating that the controller had processed personal in a manner that infringes the GDPR.

6.4 *Ex-officio* Investigations

Investigation in relation to the alleged scanning and reuse of personal data in film productions

Allegations were brought before the Commissioner concerning individuals who had been engaged as background extras on a film production and were subsequently selected at random to undergo a scanning procedure.

Among the allegations, it was claimed that the physical characteristics of these individuals were collected with the intention of further processing these data for use in future film productions.

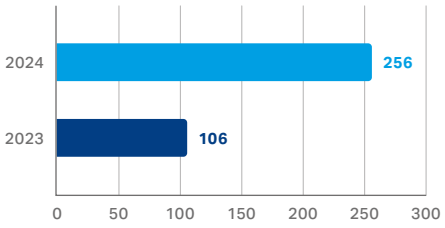
For this purpose, the Commissioner initiated an ex-officio investigation into the company established in Malta allegedly responsible for the processing of the data. However, during the course of the investigation, the Commissioner established that the company in question did not qualify as a controller within the meaning of article 4(7) of the GDPR. This determination was made on the basis that the company neither owns the device nor processes any personal data of the extras. Further investigation revealed that the controller responsible for the processing is another company based in the United Kingdom.

After further investigation, the Commissioner established that the company responsible for the processing is established in the UK. Given that the company does not fall within the territorial scope of the GDPR as it does not have an establishment in Malta or the EU within the meaning of article 3(1) of the GDPR and the company does not offer goods or services to data subjects located in the EU within the meaning of article 3(2)(a) of the GDPR nor monitors the behaviour of such data subjects within the meaning of article 3(2)(b) of the GDPR, the Commissioner did not have the competence to investigate the controller established within the United Kingdom.

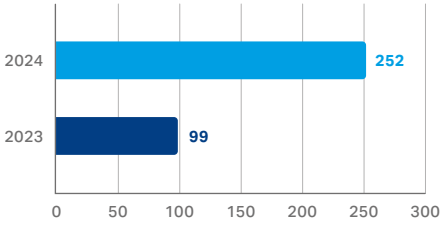
6.5 One-Stop-Shop Cases

In 2024, there were two hundred and fifty-six (256) complaints filed under the Internal Market Information (IMI) system, a substantial increase compared to the one hundred and five (105) complaints recorded in 2023. Out of these, two hundred and forty-nine (252) were LSA cases, and four (4) were CSA cases, compared to ninety-nine (99) and seven (7) cases respectively in the previous year. The most cases were received from Austria (124), followed by Germany (105), Sweden (11) and other countries receiving fewer cases.

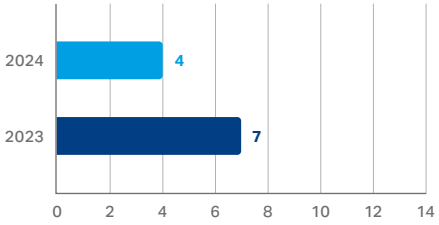
Total OSS Cases



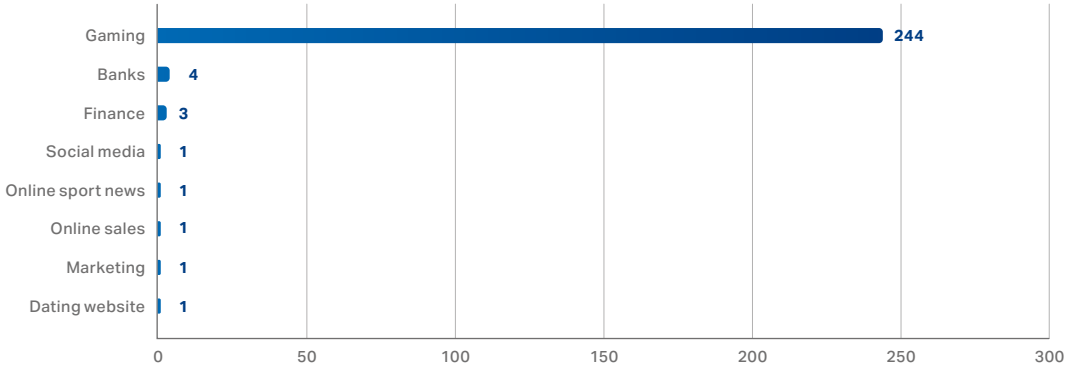
Cases acting as LSA



Cases acting as CSA



Number of Complaints by Sector

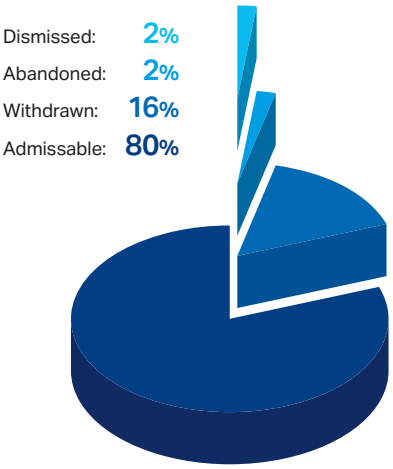


6.5 One-Stop-Shop Cases

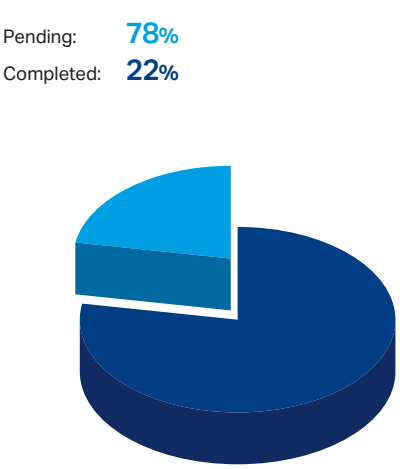
The sector with the highest number of complaints was gaming, accounting for two hundred and forty-four (244) cases, while sectors such as banks and finance counted respectively four (4) and three (3) complaints and other sectors such as dating sites, marketing, online sales, online sport news and social media had only one (1) complaint each.

Most of these complaints, two hundred and thirty-one (231) cases, were related to right of access requests, followed by eight (8) cases of right of erasure requests where other violations such unsolicited communications, disproportionate request of personal data, identity theft, security of processing and transparency had just 1 or 2 cases each. Regarding case outcomes, two hundred and six (206) complaints were deemed admissible, while five (5) were abandoned and five (5) dismissed, and forty (40) were withdrawn. Most of the investigation are pending waiting for the outcome of appeals for similar cases at a national level.

Complaints Status



Number of Cases



6.6 Personal Data Breaches

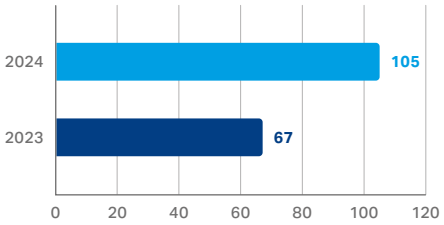
In 2024, a total of one hundred and five (105) personal data breaches were reported, marking an increase from the sixty-seven (67) breaches reported in 2023.

The sectors most affected by these breaches include other services with thirty-four (32) incidents reported followed by education with twenty-one (21) breaches, gaming with fourteen (14) and financial services with eleven (11). Lesser affected sectors included health, banks, manufacturing, wholesales, public administration and cryptocurrency with respectively seven (7), six (6), four (4), three (3) and one (1) reported breaches. Six (6) notifications were withdrawn by the controllers.

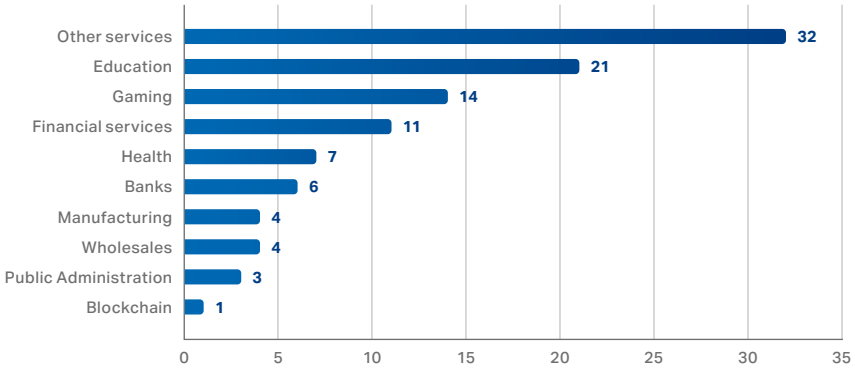
The majority of the breaches had as cause cyberattacks, including phishing attacks and ransomware attacks, which accounted for sixty-one (61) incidents. Other causes were personal data sent to wrong recipient (24 breaches), data of wrong data subject shown (6 breaches), unintended publication (5 breaches).

Less common causes were mail lost or opened, paper lost or stolen or left in insecure location, incorrect disposal of data and device lost or stolen or left in insecure location with among three (3) and one (1) breach reported.

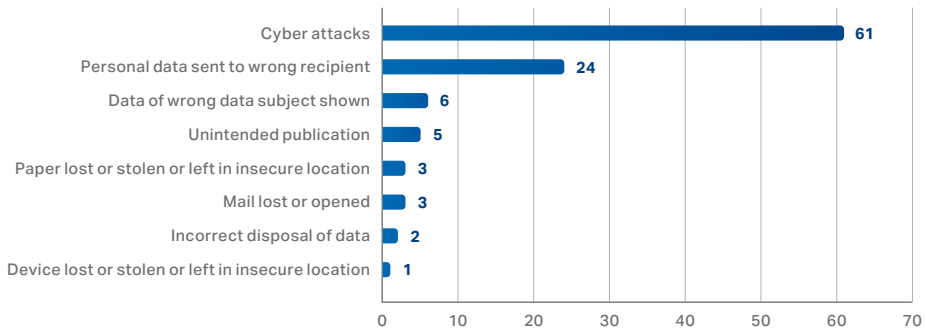
Total number of Breach Notifications received



Number of breaches by sector



Nature of the breaches

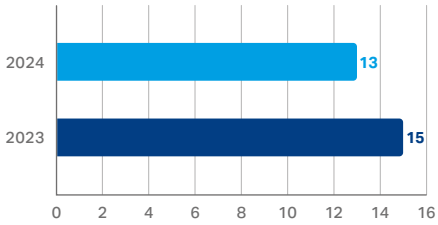


6.6 Personal Data Breaches

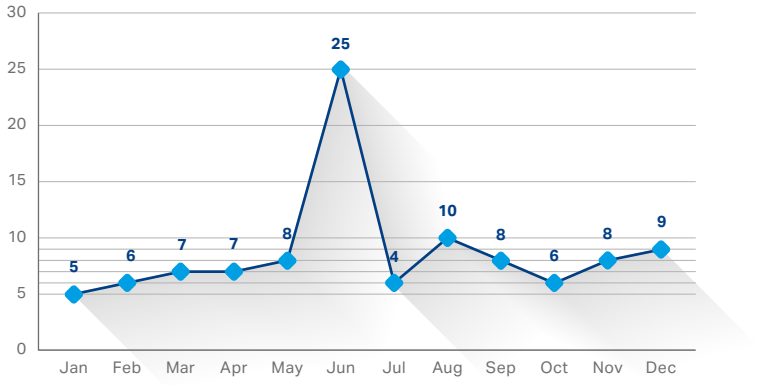
In terms of notifications received from controllers outside the EU, there was a slightly decrease from fifteen (15) in 2023 to thirteen (13) in 2024. Throughout the year, the number of breaches reported fluctuated, peaking in June with twenty-five (25) breaches reported.

The majority of cases – 82% - resulted in no action being taken, while fourteen (14) cases were concluded with instructions being issued to the controllers and in one (1) case the controller was served with a reprimand.

Number of notified breaches by controllers outside the EU



Number of breaches by month



6.7 Administrative Fine imposed by the Commissioner

On 28 June 2024, the Commissioner concluded an investigation into a data protection complaint concerning repeated unsolicited marketing communications received by a data subject, despite prior assurances from the controller that the personal data pertaining to the data subject had been erased and the mobile numbers excluded from further processing.

> **After a comprehensive investigation, the Commissioner determined that the controller had failed to uphold the data subject's right to object to direct marketing under article 21(2) of the GDPR.**

The data subject had initially raised concerns in 2022, following which the controller confirmed that the data had been deleted and the numbers barred. However, the data subjects continued to receive marketing calls and SMS messages promoting the products and services of the controller.

In response to the complaint lodged by the data subject, the controller argued that the subsequent calls were generate randomly by a software tool that selected numbers without reference to identified natural persons, and thus, this did not constitute processing of personal data. Nonetheless, the controller acknowledged this issue and stated that additional safeguards, such as a barred number list within its centralised telephone system, had since been implemented.

The data subject disputed the submissions of the controller and provided evidence of emails that include her full name, professional title, and both mobile numbers, which effectively demonstrated that her personal data remained in use. Furthermore, during the course of the investigation, the data subject continued receiving marketing calls. The controller later attributed this to subcontractors using personal devices and claimed that this was purely an oversight.

After a comprehensive investigation, the Commissioner determined that the controller had failed to uphold the data subject's right to object to direct marketing under article 21(2) of the GDPR. Additionally, the controller was found to have infringed the principle of accountability as set forth in article 5(2) of the GDPR.

In view of the persistent nature of the infringements and the controller's failure to implement effective measures over an extended period, the Commissioner imposed an administrative fine of €15,000 pursuant to article 58(2)(i) of the GDPR in order to demonstrate the seriousness and gravity of the infringements. The case was appealed by the controller.

Other administrative fines were collected in 2024 following final judgments delivered by the Information and Data Protection Appeals Tribunal and the Court of Appeal in relation to cases that were concluded by the Commissioner in previous years.

6.8 Supervisory Audits

Following the adoption of the new Schengen evaluation and monitoring mechanism Regulation (EU) No 1053/2013 of 7 October 2013, the Commission established during 2023 a pool of experts from Member States to ensure the participation of a sufficient number of experienced experts to conduct SCHEVAL inspections in a faster and less burdensome way.

This office contributed to the pool of experts by nominating its own nominees in the field of data protection. During May 2023, IDPC experts were selected to participate in the Data Protection – Schengen Evaluation of Croatia.

By virtue of Regulation (EU) 2018/1861 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006 and Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS), during 2023, this office was entrusted with the Supervisory Authority role in the field of data protection.

During 2024, audits at the SIRENE, N.SIS and Europol and EuroDac offices within the Malta Police were conducted. Additional audits and visits were carried out at the Visa Office within the Ministry for Foreign and European Affairs, at Identita', and at the Embassy of Istanbul in relation to the issuing of Visas.

These inspections follow an established yearly schedule. An audit methodology based on international standards is applied to ascertain that data protection obligations are met through the use, storage and security of both systems by the designated competent authorities in Malta.

The Coordinated Supervision Committee (CSC) is a group of national supervisory authorities and the European Data Protection Supervisor (EDPS) ensures coordinated supervision of large-scale IT systems and of EU bodies, offices and agencies. This office is part of this fora and during 2024 members of the IDPC attended regular CSC meetings at the EDPB.

07

Freedom of Information

07

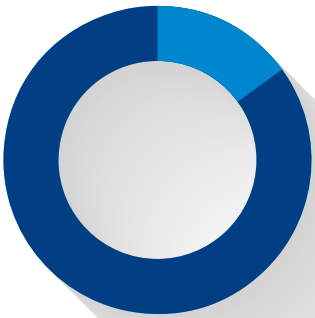
Freedom of Information

A total of seven hundred ninety-eight (798) cases were handled by public authorities during the reporting period, including 139 (one hundred thirty-nine) that were opened in 2023 and closed in 2024.

In 2024, public authorities recorded a total of six hundred fifty-nine (659) requests. Of these, two hundred eighty-four (284) were accepted, while two hundred thirty-nine (239) were not accepted. Additionally, one hundred eighteen (118) requests remained open and eighteen (18) were withdrawn.

The Lands Authority received the highest volume of requests, totalling one hundred seventy-four (174), with fifty-six (56) accepted, fifty-two (52) not accepted, fifty-four (54) still being processed and twelve (12) were withdrawn. Other significant public authorities included the Malta Police Force, which handled thirty-seven (35) cases and the Office of the Prime Minister (OPM) handing twenty-seven (27) cases. The report also highlights the average response time for first actions, which stood at twenty-eight (28) working days.

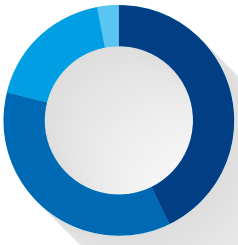
2024 Workload (798)



Cases opened in 2023 but closed in 2024: 17%

New cases Recorded in 2024 83%

Public Authorities (659 total)



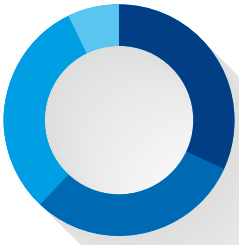
Withdrawn: 3%

Still being processed: 18%

Not accepted: 36%

Accepted: 43%

Lands Authority (174 total)



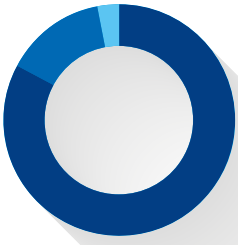
Withdrawn: 12

Still being processed: 54

Not accepted: 52

Accepted: 56

Malta Police Force (35 total)



Withdrawn: 1

Still being processed: 0

Not accepted: 5

Accepted: 29

07

Freedom of Information

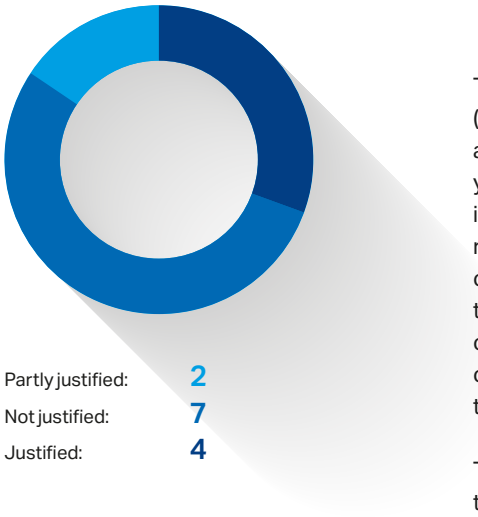
Below are the main reasons cited by public authorities for rejecting requests, along with their corresponding numbers.

Reason for Requests refused	Total
Document is withheld in terms of Part V or Part VI of the Act	**54**
Document requested is excluded from the scope of the Freedom of Information Act by virtue of Article 5	**37**
Resources required to identify, locate or collate the document or documents would substantially and unreasonably divert the resources of the authority for its operations.	**4**
The document requested cannot be found.	**5**
The document requested is not held by the Public Authority, or connected more closely with the functions of, another public authority.	**60**
The document requested is publicly available or will be published within three months.	**49**
The request is considered frivolous, trivial or vexatious.	**5**
Other reasons	**61**
Total requests refused	**275**

07

Freedom of Information

Decision Notices



Partly justified: 2
Not justified: 7
Justified: 4

This office received a total of forty-seven (47) FOI applications in 2024, reflecting a slight decrease from the previous year, when fifty-four (54) cases were investigated. Out of the applications received during the year in review, forty-one (41) were concluded. These included two (2) complaints that were dismissed, one (1) that was deemed inadmissible, one (1) that was withdrawn and one (1) that was classified as abandoned.

Thirteen (13) complaints were resolved through amicable settlement, while in six (6) cases, the public authorities adhered to the Commissioner's instructions. The Commissioner issued four (4) Decision Notices where the exemption was found to be justified, seven (7) where it was not justified and two (2) where it was partly justified.

The University of Malta (UoM) and the Malta Tourism Authority (MTA) were the most frequently investigated public authorities. The cases involving UoM were resolved through amicable settlements, reflecting successful mediation efforts to address FOI concerns without escalation. Public authorities frequently relied on specific exemptions under the FOI Act to justify withholding information. The most commonly cited exemptions included article 32(1)(c)(i) of the FOI Act, which is often invoked to prevent the disclosure of information that could unreasonably affect a person's or organisation's lawful business, commercial or financial affairs; and article 5(1)(f) of the FOI Act, which states that FOI legislation does not apply to documents held by a commercial partnership in which the Government of Malta has a controlling interest, provided the documents relate to commercial activities.

A total of six (6) FOI appeals were filed in 2024. Five (5) of these appeals were lodged by public authorities after the Commissioner ruled that the exemptions they had invoked were unjustified and ordered the release of the requested documents. One (1) appeal was filed by an applicant who contested the Commissioner's decision that a public authority was justified in withholding information.

One notable case was Rebecca Bonello Ghio vs Malta Film Commission, in which the Commissioner initially ruled that the requested documentation should be disclosed. The Malta Film Commission appealed to the Tribunal, which upheld the Commissioner's decision. The case then proceeded to the Court of Appeal, which also ruled in favour of the applicant, confirming the Public Authority's obligation to release the information. As a result, the court ordered the Malta Film Commission to disclose the amount paid to British comedian and author David Walliams for hosting the Malta Film Awards in January 2022. The judgment reaffirmed that public authorities cannot invoke confidentiality agreements to conceal financial expenditures, echoing earlier rulings by the Commissioner and the Tribunal. The Malta Film Commission had previously refused other FOI requests citing professional privilege and confidentiality clauses; however, both the Commissioner and the Tribunal found these claims unjustified. The court emphasised the duty of public authorities to uphold transparency and accountability, particularly when handling taxpayer funds and ordered the disclosure of electronic copies of the invoices related to Walliams' payment.

08

Litigation

08

Litigation

The Commissioner is frequently summoned to appear before the Information and Data Protection Appeals Tribunal as well as the Courts of Justice, either to provide testimony or submit documentation in connection with data protection complaints and freedom of information requests investigated by this office. At times, judicial proceedings are also instituted against the Commissioner in the exercise of his statutory functions. Conversely, the Commissioner may also initiate appeals before the Courts of Justice when contesting decisions delivered by the Information and Data Protection Appeals Tribunal which, in his view, misinterpret or misapply the relevant legal framework. These proceedings form an essential part of the broader legal and institutional framework for the enforcement and protection of fundamental rights relating to data protection and access to information.

During 2024, the Commissioner was involved in the following judicial proceedings:

- **Prof Ivan Sammut vs Avukat tal-Istat et, First Hall Civil Court (Constitutional Jurisdiction)**

  The First Hall Civil Court (Constitutional Jurisdiction) delivered its judgment on 27 September 2023 and decided to dismiss the case on the basis that the plaintiff did not exercise any of the ordinary remedies provided by law, which includes inter alia, the right to lodge a complaint with the Commissioner pursuant to article 77(1) of Regulation (EU) 2016/679. Prof Sammut has appealed the decision, and the case is currently pending before the Court of Appeal.

- **Nutar Dr Robert Aquilina vs Avukat tal-Istat et, First Hall Civil Court (Constitutional Jurisdiction)**

  The case was initiated in 2022 and remains ongoing as of 2024. The parties are currently expected to submit their respective notes of submissions.

- **Environmental Landscapes Consortium Limited vs Il-Kummissarju għall-Informazzjoni u l-Protezzjoni tad-Data u l-Ministru għat-Trasport u l-Infrastruttura (Court of Appeal)**

  This FOI case concluded with a judgement delivered on 30 July 2024. The Court of Appeal overturned the initial decision and remitted the case to the First Court for a fresh hearing, ordering that the applicant be summoned to appear.

- **Rebecca Bonello vs National School Support Services (NSSS) (Court of Appeal)**

  On 4 May 2023, following receipt of a complaint alleging that the controller providing speech and occupational-therapy services at the complainant's son's school had acted in contravention of the Regulation, the Commissioner issued a decision upholding those allegations. The Information and Data Protection Appeals Tribunal subsequently reversed the Commissioner's ruling. The Commissioner thereupon lodged an appeal against the Tribunal's judgment, and on 6 November 2024, the Court of Appeal reinstated the Commissioner's decision in its entirety, thereby confirming the controller's non-compliance with the Regulation.

09

Financial Statements

Office of the Information and Data Protection Commissioner

Annual Report and Financial Statements

For the Year Ended 31 December 2024

Office of the Information and Data Protection Commissioner

For the Year Ended 31 December 2024

Contents

Office of the Information and Data Protection Commissioner

Commissioner's Report

For the Year Ended 31 December 2024

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 2024.

General Information

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

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.

Results

During the year, the Authority registered a surplus of €49,720 (2023: a surplus of €1,308). The Authority received Government subvention amounting to €750,000 in 2024, representing an increase of 7% when compared to 2023. Total administrative expenditure amounted to €704,500, resulting in an increase of 2% when compared to 2023. 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 2024, the Authority did not collect any notification fees (2023: Nil).

The results for the year are set out on in the Statements of Profit or Loss and Other Comprehensive Income on page 5.

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 made available by the Government of Malta through the subventions to enable the Authority to meet its commitments as and when they fall due.

Principal Risks and Uncertainties

The Authority's activities expose it to a variety of financial risks: liquidity risk, fair values risk and capital risk management. The Authority's overall risk management programme focuses on the unpredictability of financial markets and seeks to minimise potential adverse effects on the Authority's financial performance.

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, 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.

Commissioner

The present Commissioner who held office during the year was:

Mr. Ian Deguara

In accordance with article 11 of the Data Protection Act, CAP. 586 of the Laws of Malta, the Commissioner is appointed by the Prime Minister after having consulted with the Leader of the Opposition. The Commissioner is appointed for a period of five years, with effect from 21 December 2020.

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 as adopted by the European Union;
- 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 30 June 2025 and signed by:

_____

Mr. Ian Deguara
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 18 which comprise the statement of financial position as at 31 December 2024, the Statements of Profit or Loss and Other 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 significant accounting policies.

In our opinion, the accompanying financial statements give a true and fair view of the financial position of the Authority as at 31 December 2024, and of its financial performance for the year then ended in accordance with International Financial Reporting Standards as adopted by the European Union and have been properly prepared in accordance with the requirements of the Data Protection Act (Cap. 586).

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 Commissioner's report and schedule. Our opinion on the financial statements does not cover the other information and we do not express any form of assurance conclusion thereon. 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.

In addition, in light of the knowledge and understanding of the Authority and its environment obtained in the course of the audit, we are required to report if we have identified material misstatements in the Commissioner's report and other information. We have nothing to report in this regard.

Responsibilities of the Commissioner

The Commissioner is responsible for the preparation of the financial statements that give a true and fair view in accordance with International Financial Reporting Standards as adopted by the European Union, and 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.

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.

- Obtain sufficient appropriate audit evidence regarding the financial information of the Authority or its operating activities to express an opinion on the consolidated financial statements.

We also provide those charged with governance with a statement that we have complied with relevant ethical requirements regarding independence, and to communicate with them all relationships and other matters that may reasonably be thought to bear on our independence, and where applicable, related safeguards.

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

30 June 2025

Office of the Information and Data Protection Commissioner

Statements of Profit or Loss and Other Comprehensive Income

For the Year Ended 31 December 2024

	Note	2024	2023
		€	€
Government subvention		750,000	700,000
Administrative expenses		(704,500)	(690,711)
Operating surplus		45,500	9,289
Finance costs		(8,541)	(9,265)
Loss on disposal		(239)	-
Other income		13,000	1,284
Surplus for the year	3.	**49,720**	**1,308**

The notes on pages 9 to 18 form an integral part of these financial statements.

Office of the Information and Data Protection Commissioner

Statement of Financial Position

As at 31 December 2024

	Note	2024 €	2023 €
ASSETS			
Non-current assets			
Property, plant and equipment	6.	251,442	290,079
Current assets			
Trade and other receivables	7.	1,581	1,590
Cash and cash equivalents	8.	300,485	262,515
Total current assets		302,066	264,105
TOTAL ASSETS		553,508	554,184
EQUITY AND LIABILITIES			
Equity			
Retained Funds		200,383	150,663
Liabilities			
Non-current liabilities			
Lease liabilities	9.	236,659	263,408
Current liabilities			
Lease liabilities	9.	26,749	25,959
Trade and other payables	10.	89,717	114,154
Total current liabilities		116,466	140,113
TOTAL EQUITY AND LIABILITIES		553,508	554,184

The notes on pages 9 to 18 form an integral part of these financial statements.

These financial statements on pages 5 to 18 were approved by the Office of the Information and Data Protection Commissioner on 30 June 2025 and were signed on its behalf by:

_____

Mr. Ian Deguara
Commissioner

Office of the Information and Data Protection Commissioner

Statement of Changes in Equity

For the Year Ended 31 December 2024

	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
Balance as at 01 January 2023	149,355	149,355
Surplus for the year	1,308	1,308
Balance as at 31 December 2023	150,663	150,663

The notes on pages 9 to 18 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 2024

	Note	2024 €	2023 €
Cash from operating activities:			
Surplus for the year		49,720	1,308
Interest expense	9.	8,541	9,265
Depreciation and amortisation	6.	39,695	43,493
Loss on disposal of property, plant and equipment		239	-
Profit from operations		98,195	54,066
Movement in trade and other receivables		9	(49)
Movement in trade and other payables		(24,436)	32,606
Net cash flows from operating activities		73,768	86,623
Cash flows from investing activities:			
Payments for property, plant and equipment	6.	(1,498)	(7,731)
Disposal of property, plant and equipment		200	-
Net cash flows used in investing activities		(1,298)	(7,731)
Cash flows from financing activities:			
Repayment of finance lease liabilities	9.	(34,500)	(32,600)
Net cash flows used in financing activities		(34,500)	(32,600)
Net cash from cash and cash equivalents		37,970	46,292
Cash and cash equivalents at beginning of year		262,515	216,223
Cash and cash equivalents at end of year	8.	300,485	262,515

The notes on pages 9 to 18 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 as adopted by the European Union.

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 International Financial Reporting Standards as adopted by the European Union 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 2024. 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 issued 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 made available by the Government of Malta through the subventions to enable the Authority to meet its commitments as and when they fall due.

2. Significant 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.

b. Property, plant and equipment

i. Value method

Items of property, plant and equipment are measured 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:

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.

c. 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.

2. Significant Accounting Policies (Continued)

c. Impairment of non-financial assets (Continued)

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.

d. 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

Except for those trade receivables that do not contain a significant financing component and are measured at the transaction price in accordance with IFRS 15, all financial assets are initially measured at fair value adjusted for transaction costs (where applicable).

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. Significant Accounting Policies (Continued)

d. Financial instruments (Continued)

iv. Impairment of financial assets

IFRS 9's impairment requirements use more forward-looking information to recognise expected credit losses - the 'expected credit loss (ECL) model'. This replaces IAS 39's 'incurred loss model'. Instruments within the scope of the new requirements included loans and other debt-type financial assets measured at amortised cost and FVOCI, trade receivables, contract assets recognised and measured under IFRS 15 and loan commitments and some financial guarantee contracts (for the issuer) that are not measured at fair value through profit or loss.

Recognition of credit losses is no longer dependent on the Authority's first identifying a credit loss event. Instead, the Authority considers a broader range of information when assessing credit risk and measuring expected credit losses, 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 expected credit losses' are recognised for the first category while 'lifetime expected credit losses' are recognised for the second category.

Measurement of the expected credit losses is determined by a probability-weighted estimate of credit losses over the expected life of the financial instrument.

v. Classification and measurement of financial liabilities

As the accounting for financial liabilities remains largely the same under IFRS 9 compared to IAS 39, the Authority's financial liabilities were not impacted by the adoption of IFRS 9. However, for completeness, the accounting policy is disclosed below.

The Authority's financial liabilities include trade and other payables. 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).

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.

2. Significant Accounting Policies (Continued)

e. Trade and other receivables

Trade and other receivables are recognised initially at fair value and subsequently measured at amortised cost using the effective interest method, less provision for impairment. A provision for impairment of trade receivables is established when there is objective evidence that the Authority will not be able to collect all amounts due to the original terms of the receivables.

f. Cash and cash equivalents

Cash and cash equivalents comprises of cash in hand and bank balances.

g. Provisions and contingent liabilities

A provision is recognised when, as a result of a past event, the Authority has a present obligation that can be estimated reliably and it is probable that the Authority will be required to transfer economic benefits in settlement. Provisions are recognised as a liability in the balance sheet and as an expense in profit or loss or, when the provision relates to an item of property, plant and equipment, it is included as part of the cost of the underlying assets.

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.

h. 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. 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.

i. Trade and other payables

Trade and other payables are stated at cost, which approximates fair value due to the short-term nature of these liabilities.

j. Revenue recognition

The Office of the Information and Data Protection Commissioner 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.

2. Significant Accounting Policies (Continued)

k. Foreign currencies

Transactions denominated in foreign currencies are converted to the functional currency at the rates of exchange ruling on the dates on which the transactions first qualify for recognition. Monetary assets and liabilities denominated in foreign currencies at the reporting date are retranslated to the functional currency at the exchange rate at that date. The foreign currency gain or loss on monetary items is the difference between amortised cost in the functional currency at the beginning of the period, adjusted for effective interest and payments during the period, and the amortised cost in foreign currency translated at the exchange rate at the end of the period. Foreign currency differences arising on retranslation are recognised in profit or loss.

l. 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.

m. Financial risk management

The exposures to risk and the way risks arise, together with the Authority's objectives, policies and processes for managing and measuring these risks are disclosed in more detail below. The objectives, policies and processes for managing financial risks and the methods used to measure such risks are subject to continual improvement and development.

i. Foreign exchange risk

The Authority is exposed to foreign exchange risk arising from various currency exposure, primarily with respect to the US dollar and the UK pound. Foreign exchange risk arises from future commercial transactions, recognised assets and liabilities and net investments in foreign operations.

ii. Liquidity risk

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.

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 8. and items presented within the retained funds in the statement of financial position.

3. Surplus for the year

Surplus for the year is charged after charging the following:

	2024	2023
	€	€
Audit fees	2,750	2,499
Depreciation expense	39,695	43,493
Total	42,445	45,992

4. 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.

5. Staff costs

a. Wages and salaries

Payroll costs for the year comprise of the following:

	2024	2023
	€	€
Salaries and wages	465,989	483,854
Social security contributions	29,650	30,694
Total	495,639	514,548

b. Number of employees

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

	2024	2023
	No.	No.
Commissioner	1	1
Directly employed by the Office	10	10
Total	11	11

6. 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	68,931	7,294	528,530
Additions	-	-	-	1,498	-	1,498
Disposals	-	-	-	(4,393)	-	(4,393)
Balance at 31 December 2024	362,719	72,186	17,400	66,036	7,294	525,635
Depreciation						
Opening balance	(98,923)	(53,246)	(17,400)	(63,925)	(4,957)	(238,451)
Charge for the year	(32,975)	(3,193)	-	(2,748)	(779)	(39,695)
Depreciation released on disposal	-	-	-	3,953	-	3,953
Balance at 31 December 2024	(131,898)	(56,439)	(17,400)	(62,720)	(5,736)	(274,193)
Net Book Value						
At 31 December 2023	263,796	18,940	-	5,006	2,337	290,079
At 31 December 2024	230,821	15,747	-	3,316	1,558	251,442

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 shall be applicable 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*.

7. Trade and other receivables

	2024	2023
	€	€
Notification fee receivables (note i)	-	222,374
Provision for doubtful debts for notification fees (note i)	-	(222,374)
Prepayments	1,581	1,590
Total	1,581	1,590

(i) In the current financial year, the Authority wrote off bad debts amounting to €222,374. Since the amount was previously recognised as an expected credit loss, the write-off had no impact on profit or loss in the current year.

8. Cash and cash equivalents

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

	2024	2023
	€	€
Cash on hand	427	982
Bank balances	300,058	261,533
Total cash and cash equivalents in the statement of cash flows	300,485	262,515

9. Lease liabilities

a. Amounts recognised in the statement of financial position

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

	2024	2023
	€	€
Right-of-use assets		
Buildings	230,821	263,796
Lease liabilities		
Current	26,749	25,959
Non-current	236,659	263,408
Total	263,408	289,367

The maturity of lease commitments is analysed as follows:

	2024	2023
	€	€
Less than one year	26,749	25,959
Between one and five years	127,843	120,158
More than five years	108,816	143,250
	263,408	289,367

9. Lease liabilities (Continued)

b. Amounts recognised in the statements of profit or loss and other comprehensive Income

Statements of profit or loss and other comprehensive Income shows the following amounts relating to leases:

	2024	2023
	€	€
Amortisation of right-of-use assets	32,975	32,975
Interest expense	8,541	9,265

The total cash outflow of the Authority for leases during the year ended 31 December 2024 is €34,500 (2023: €32,600).

10. Trade and other payables

	2024	2023
	€	€
Trade payables	1,925	2,493
Amount payable to related parties (Note 12.)	81,047	78,547
Accruals	6,745	33,114
Total	89,717	114,154

The amount payable to related parties is unsecured, interest free and repayable on demand.

11. 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 is valid until 1st July 2025. The guarantee is callable by the Authority in the event of non-performance or breach of contract by the counterparty. No amounts have been recognized in respect of this guarantee as at the year ended, as no default has occurred.

12. 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 10.