2022

ANNUAL REPORT

idpc.
INFORMATION AND DATA PROTECTION COMMISSIONER


idpc.
INFORMATION AND DATA
PROTECTION COMMISSIONER

CONTENTS

FOREWORD

I have the pleasure to share with you the report prepared for the year 2022 which presents the principal regulatory activities which we have undertaken during the period. It was indeed a busy year: twelve calendar months during which progress has been achieved on several strategic matters.

During the year under review, we have issued legally binding decisions issued on significant cases. Two of these decisions involve personal data incidents that were notified to our office in 2020 by two separate controllers operating in the information technology and gaming sectors respectively. Given the serious nature of the breaches, an administrative fine of €65,000 and €250,000 was the most appropriate corrective measure to be imposed on the responsible controllers. Both decisions have been appealed before the Information and Data Protection Appeals Tribunal.

On an EU level, in April, EEA data protection authorities met in Vienna for a two-day high-level meeting and agreed to further enhance cooperation on strategic cases, and to diversify the range of cooperation methods used. More than ever, strong and swift enforcement is crucial for ensuring a consistent interpretation of the GDPR. As Commissioners we have reiterated our commitment to close cross-border cooperation and agree to further enhance it in the following manner. The main outcome of this meeting was that

supervisory authorities will collectively identify cross border cases of strategic importance in different Member States on a regular basis, for which cooperation will be prioritised and supported by EDPB.

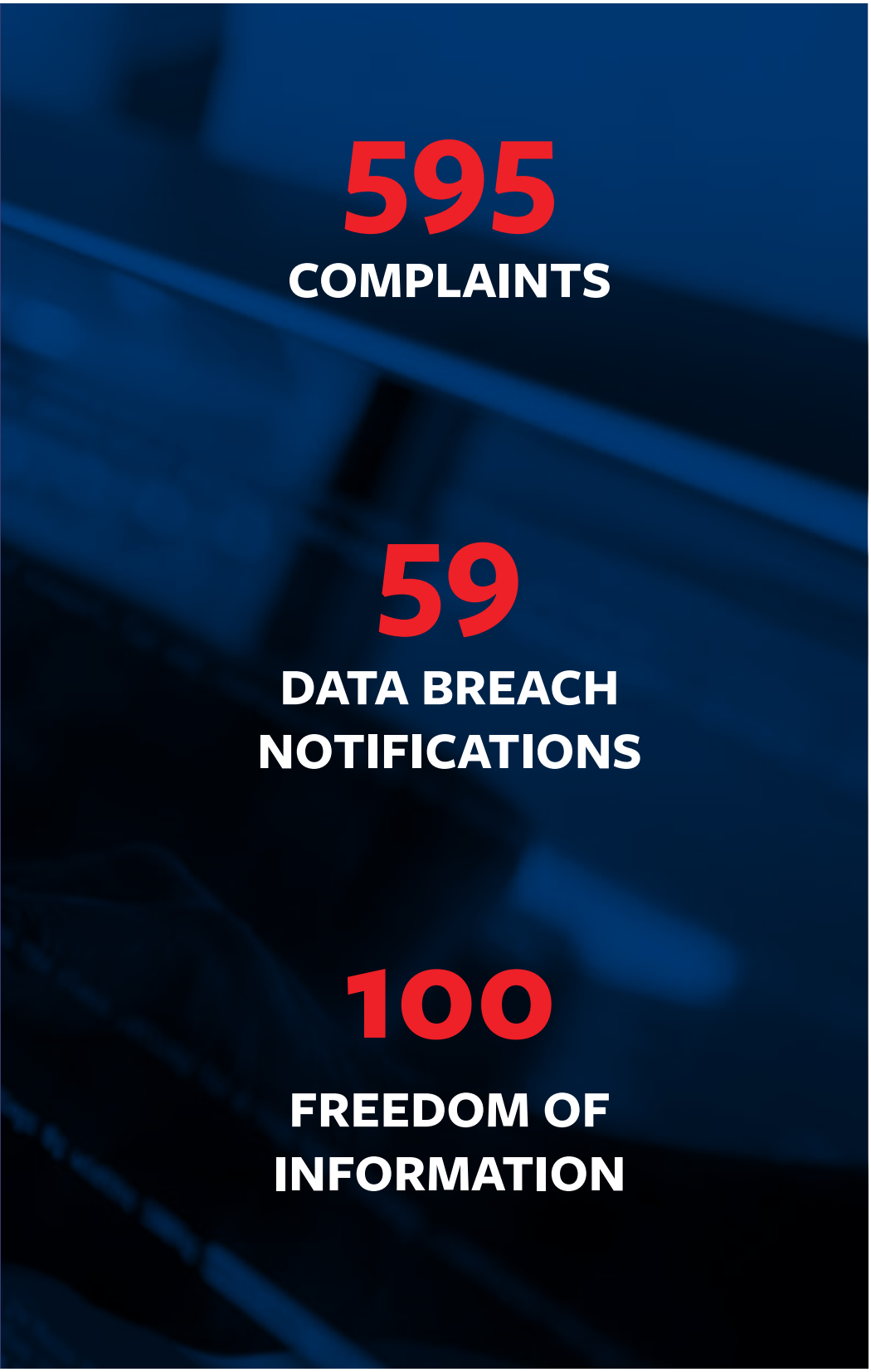
During 2022, the decision notices issued by our office on the FOI applications concerning the same subject manner, namely the interpretation of the term document as defined in the Freedom of Information Act, were appealed by almost all the public authorities which were subject to this notice. We look forward to see the outcome of this process given that the interpretation of this specific term is fundamental to the application of the open government legislation.

I am profoundly honoured to head the data protection authority in this journey and am committed to invest in my structured efforts, together with my team, to continue upholding the data protection rights of individuals against any form of unlawful processing. We are equally committed to preserve our thorough and speedy analysis in the investigation of freedom of information cases as these decisions keep public authorities in check in terms of ensuring accountability and transparency in their operations.

Ian Deguara

Information and Data Protection Commissioner

YEAR 2022 AT A GLANCE


595
COMPLAINTS
59
DATA BREACH NOTIFICATIONS
100
FREEDOM OF INFORMATION

OUR OFFICE

2.1 Our Mission and Vision

The Office of the Information and Data Protection Commissioner (IDPC) is the independent supervisory authority responsible for monitoring and enforcing the General Data Protection Regulation and the Data Protection Act (Cap. 586 of the Laws of Malta), including the regulations made thereunder. The IDPC is also responsible for promoting the observance by the relevant public authorities of the requirements of the Freedom of Information Act (Cap. 496 of the Laws of Malta).

The mission of the IDPC is to ensure a high level of protection to the rights and freedoms of natural persons.

2.2 Our strategic objectives

By performing its tasks and duties, the IDPC aims at:

- introducing a culture where safeguarding data protection rights is perceived as a natural process that forms an integral part of organisations' operations, rather than a legal burden;
- increasing the level of trust by the general public that their personal data is used in accordance with the requirements of data protection legislation;
- enforcing data protection legislation by taking appropriate corrective action against controllers and processors which are found infringing the law;
- assisting SMEs in complying with the data protection legislation;
- taking initiatives to raise data protection awareness, also making use of dedicated EU funds to achieve this objective;
- communicating extensively with stakeholders;
- contributing to the consistent application of the General Data Protection Regulation by cooperating with its European counterparts through the consistency mechanism and participating as active member to European Data Protection Board fora; and
- ensuring transparency and good governance by public authorities.

2.3 Staff compliment and Budget

In 2022, the IDPC retained the same number of full-time employees like the previous year. The staff complement consists of 15 members of staff having both legal and technical skills and competences. In 2023, the IDPC is foreseeing to strengthen the technical team and also to create a communications function within the office.

The total budget allocated for the IDPC for the year under review was €680,000. This was an increase of €60,000 over the subvention allocated for the previous year. The consistent increases in the office's budget year on year is indeed positive and the Commissioner is committed to continue presenting concrete financial plans to the Government so that the budget allocations for 2023 and for the following years will keep on growing steadily.

3 ENGAGEMENTS

3.1 Local Engagements

3.1.1 Data Protection Day

Back in 2006 the Council of Europe decided to launch a Data Protection Day to be celebrated each year on 28 January, the date on which the Council of Europe's data protection convention, known as "Convention 108", was opened for signature. Data Protection Day is now celebrated globally.

To mark Data Protection Day, the IDPC carried out activities to raise awareness about the right to personal data protection, including an address to all Data Protection Officers appointed within the public sector during a virtual session organised by the Data Protection Unit within the Ministry for Justice, Equality and Governance. Special focus was made on the implementation of the General Data Protection Regulation (GDPR) with reference to the techniques of data pseudonymisation and anonymisation.

3.1.2 EU-funded GDPR awareness campaign

One of the statutory duties of the IDPC is to promote public awareness and understanding of the risks, rules, safeguards and rights in relation to data protection. Apart from this, the IDPC receives regular requests for advice by controllers, which portray the national need for increased awareness and assistance in complying with data protection law. For these reasons, the IDPC decided to develop an awareness project called "GDPR awareness campaign and support to business organisations, in particular, SMEs – GDPRights" after having obtained EU funds in 2019 under the Rights, Equality and Citizenship Programme 2014-2020.

As part of this initiative, during Year 2021, the IDPC issued a public tender for the design and, development of an Online Self- Assessment Compliance Tool, complete with sample reports and templates designed specifically for the use by Small to Medium Enterprises (SMEs) in their bid to increase businesses' compliance with the GDPR. The tool was eventually completed and launched during March 2022. As a result, during 2022, the amount of basic GDPR queries deriving from SME's has decreased, whilst queries related to the implementation of GDPR standards has increased.

Throughout the project the IDPC sought the assistance of relevant authorities, including the Malta Chamber of SMEs, the Malta Employers Association, the Gozo Business Chamber, the Foundation for Information Technology Accessibility.

The Online Self-Assessment Compliance Tool is available to be freely used through the IDPC official webpage (https://idpc.org.mt/for-organisations/self-assessment-compliance-tool/)

Online Self-Assessment Compliance Tool (*Main page*)

3.2 International Engagements

3.2.1 International cooperation with data protection authorities in third countries

In terms of Article 50 of the GDPR, supervisory authorities shall take appropriate steps to develop international cooperation mechanisms, inter alia, to facilitate the effective enforcement of the data protection law, provide international mutual assistance in the enforcement of data protection rules and promote the exchange of information concerning data protection legislation and practices.

In his constant drive to put into practice this legal provision, during the year under review, he signed a cooperation agreement with two data protection

authorities, namely the Gibraltar Regulatory Authority (GRA) and the Information and Data Protection Commissioner of the Republic of Albania.

The memorandum of understanding with the Information Commissioner of the GRA was signed in the margins of the 44th Global Privacy Assembly hosted by the Turkish Data Protection Authority in Istanbul from 25th to 28th October 2022.

The GRA and the IDPC, which are both members of the BIIDPA (British, Irish and islands data protection authorities) network, enjoy a longstanding relationship which the recently signed memorandum will strengthen even further, in the interest of businesses and individuals. The memorandum introduced a number of collaboration mechanisms such as exchange of best practices and mutual assistance by means of which the two authorities expect to streamline their respective regulatory duties. *1

The other cooperation agreement was signed on the margins of the 69th Plenary meeting of the European Data Protection Board, which took place in Brussels on the 12th September 2022. Under the cooperation agreement, the IDPC and the Information and Data Protection Commissioner of Albania intend to mutually exchange best practices, information and expertise in view of facilitating the application and enforcement of data protection law in their respective jurisdictions.

These agreements are a great way how data protection authorities in the EEA consolidate their relationship with their counterparts in third countries and certainly constitute the right step in enhancing international outreach in a global economy where the exchange of personal data across borders grows on a daily basis.*2

3.2.2 Meeting of all the DPAs in Vienna

During this year, the IDPC participated in a pivotal two-day high-level meeting held in Vienna, where members of the European Data Protection Board (EDPB) discussed the advancement of cooperation on strategic cases and the diversification of cooperation methods. Highlighting the urgency of robust and expeditious enforcement, the discussions underlined the imperative of ensuring a consistent interpretation of the GDPR. Andrea Jelinek, Chair of the European Data Protection Board, said: “In

*1

*2

the past four years, we have invested a great deal of resources in the interpretation and consistent application of the GDPR by endorsing and adopting no less than 57 Guidelines and 6 Recommendations. Enforcement by the data protection authorities (DPAs) has ramped up with cumulative fines adding up to 1.55Bn€ at the end of 2021. More than ever, strong and swift enforcement is crucial for ensuring a consistent interpretation of the GDPR. To stay on top of this growing workload and make the most efficient use of the possibilities for cooperation foreseen in the GDPR, we will yearly identify a number of cross-border cases of strategic importance for which an action plan with a fixed timeline for cooperation will be set. All EDPB Members are committed to close cooperation and we focus on practical solutions to strengthen the capacity of DPAs to enforce". Furthermore, the DPAs commit to exchange insights on national enforcement strategies aligning them with annual enforcement priorities at the EDPB level. In pursuit of greater harmonisation, DPAs aim to develop a common enforcement framework, inclusive of shared inspection instruments. Finally, the EDBP stressed the importance of further harmonisation of national procedural laws.

3.2.3 30th European Conference of Data Protection Authorities (Spring Conference)

The IDPC participated in the 30th European Conference of Data Protection Authorities (Spring Conference) in Dubrovnik, Croatia on the 19th to 20th May 2022. This Spring Conference brough together representatives from data protection authorities across Europe to deliberate on crucial issues surrounding the protection of personal data. Hosted by Croatia's Personal Data Protection Authority (AZOP), the Conference marked significant milestones, including the adoption of resolutions aiming to expedite the ratification process of Convention 108+ and the adoption of a second Resolution on the Conference Vision, Mission and Steering Group for the Spring Conference.

3.2.4 The Future of Data Protection: Effective Enforcement in the Digital World (EDPS Conference)

On the 16th and 17th June 2022, the IDPC participated in a pivotal conference alongside leading academics, activists, practitioners, regulators and policy-makers. Esteemed

speakers like Max Schrems of NOYB and Wojciech Wiewiórowski from the European Data Protection Supervisor (EDPS) delivered keynote speeches, setting the tone for discussions on the future of data protection. With over hundred distinguished speakers offering diverse perspectives, sixteen breakout sessions, workshops and more, the two-day conference of the EDPS fostered crucial conversations on the future of data protection. In his keynote address, Wiewiórowski accentuated the necessity of a pan-European data protection enforcement model to uphold fundamental rights consistently across the EU. He stated, "Such a model would not only mitigate the problem of uneven allocation of responsibilities, but would also help to ensure real consistency in data protection law across the EU, including through strong mechanisms of collegiality. With full respect to the principle of subsidiarity, key investigations, based on a certain threshold, the modalities of which should be further discussed, could be conducted at a central level. This would also aid in overcoming potential issues stemming from incompatible national legislation or patchwork harmonisation attempts."

3.2.5 British, Irish and Islands Data Protection Authorities (BIIDPA) Meeting

In July 2022, the UK ICO hosted the BIIDPA in London, marking the launch of its 25-year strategic plan. The participating authorities discussed key developments and exchanged ideas and action plans to facilitate regulatory progress and foster coordinated efforts. Discussions encompassed regulatory collaboration with sectorial bodies, the prioritisation of case handling, effective enforcement in the public sector, privacy awareness initiatives and promoting compliance through enhanced accountability measures. Significance importance was placed on leveraging technological and investigative expertise to identify and mitigate data protection risks, outlining the practical importance and impact of data protection to prioritise regulatory action. The Meeting concluded with the decision for the IDPC to host the next meeting in Malta.

3.2.6 Global Privacy Assembly

The IDPC participated in the 44th Global Privacy Assembly (GPA), hosted by the Personal Data Protection Authority of Turkey (KVKK) in Istanbul Turkey, from the 25th to the 28th October 2022. The GPA assembled over one hundred and thirty data protection and privacy authorities worldwide, fostering invaluable connections and insightful exchanges on the evolving landscape of data protection and the key elements of their international cooperation. Under the overarching theme, 'A Matter of Balance: Privacy in The Era of Rapid Technological Advancement', discussions delved into pressing issues such as artificial intelligence, facial recognition technologies, regulatory effectiveness, cross-border data transfers and safeguarding children's privacy.

4 ADVISORY

4.1 Consultation

The IDPC provided guidance and observations on various legislative measures in 2022 covering different sectors, which include inter alia, social accommodation, fisheries, health and electoral law.

The IDPC was also consulted on the legislation in relation to the Enforcement of the Rights of Data Subjects in relation to International Transfers outside the EU. The objective of the regulations is to apply Council Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

The IDPC aims to advance data protection by design, safeguard data protection rights and ensure the implementation of appropriate technical and organisational measures at the stage of consultation.

4.2 Advice on Queries

Throughout the year 2022, the demand for our advisory services in assisting organizations and the public remained consistently high as adhering to data protection laws poses a rigorous challenge for controllers and processors, necessitating a solid grasp of relevant legal provisions to commence this endeavour. Concurrently, data subjects must understand their rights, anticipate the handling of their data by controllers or processors, and make informed decisions accordingly.

The IDPC advocates for the openness, transparency, and inclusivity of data protection supervisory authorities' work. For this reason, the IDPC offers accessible support through an open telephone line during business hours and a general mailbox for inquiries related to data protection and freedom of information. These services cater to individuals, professionals, organizations, and public entities.

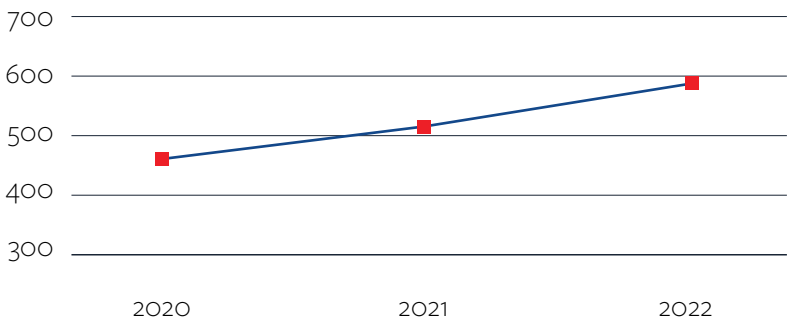
The public is being encouraged to utilize these services and the IDPC eagerly welcomes suggestions for improvement.

5 SUPERVISORY AND ENFORCEMENT ACTIVITIES

5.1 Local Data Protection Complaints

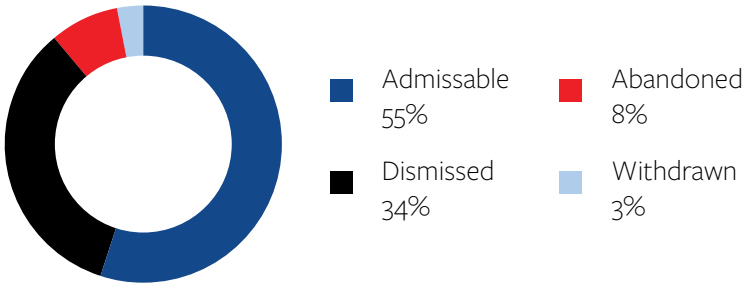
In 2022, the IDPC experienced a significant increase in local cases compared to previous years, with a total of five hundred and ninety-five (595) cases received, marking a notable rise from five hundred and nine (509) cases in 2021 and four hundred and seventy (470) cases in 2020.

Complaint comparison by year



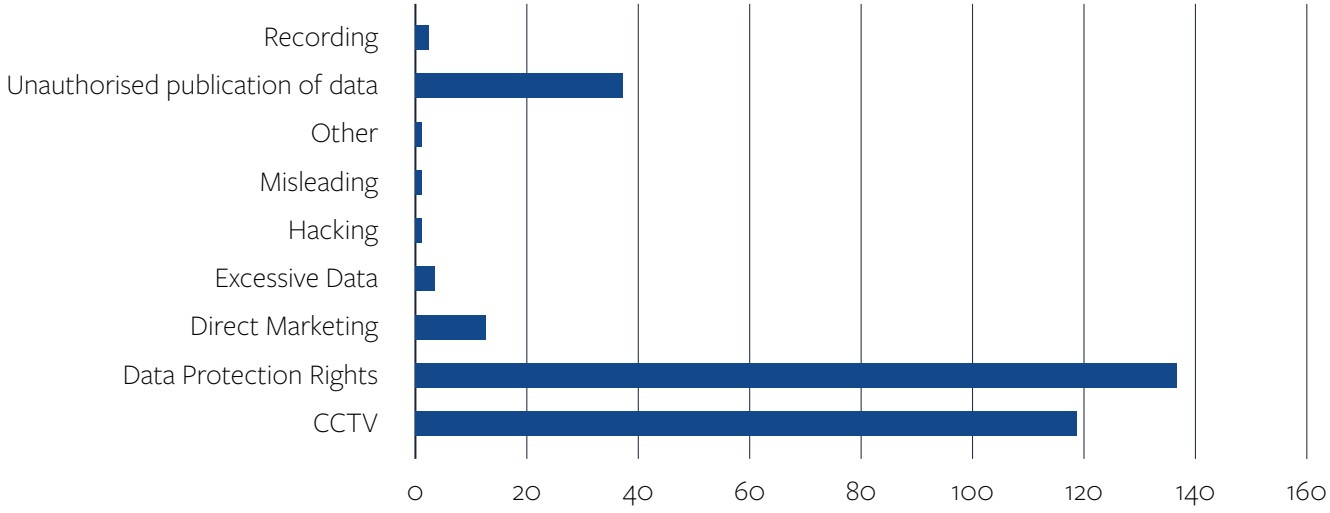
A detailed breakdown of the five hundred and ninety-five (595) cases reveals that while three hundred and twenty-six (326) cases were deemed admissible, two hundred and four (204) cases were dismissed, nineteen (19) were voluntarily withdrawn and forty-six (46) were abandoned. A notable proportion of the admissible cases, specifically two hundred and eighty (280), were successfully closed, however, forty-six (46) cases remain under investigation.

Complaints investigated during 2022



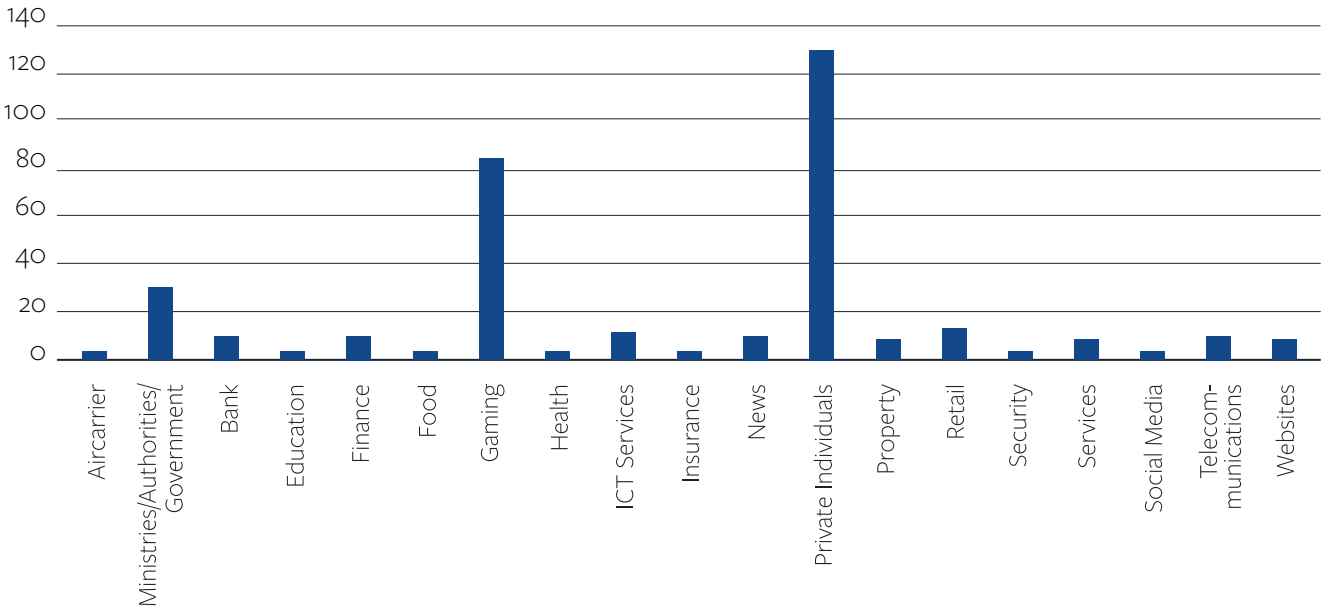
Complaints regarding the right of access were predominant, comprising the majority of the caseload, and following closely were complaints related to the processing of personal data through video-surveillance devices (CCTV).

Subject for admissible cases



The breakdown of complaints by sector revealed a consistent trend from the previous year, with private individuals and gaming companies emerging as the primary controllers under scrutiny.

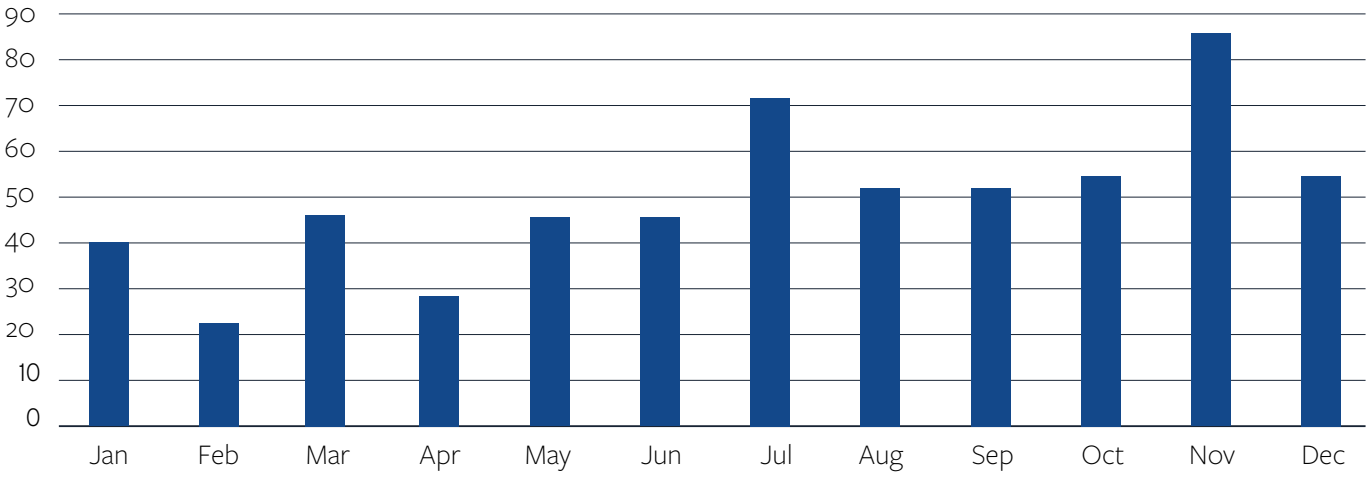
Subject for admissible cases



In terms of outcomes, the Office issued a total of two hundred and eighty (280) legally binding decisions. Among these, ninety-seven (97) decisions identified infringements, prompting corrective actions and penalties as necessary. The Commissioner imposed a total of three hundred thirty-seven thousand, five hundred euro (€337,500) in administrative fines as corrective action. Conversely, one hundred and eighty-three (183) decisions found no infringement.

The monthly distribution of complaints in 2022 exhibited fluctuations, with notable peaks in July and November, coinciding with seventy-one (71) and eighty-five (85) complaints, respectively.

Complaints received by month



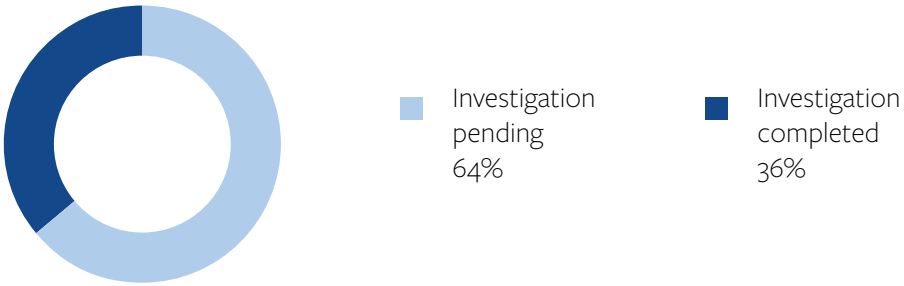
5.2 Cross-border Cases

In 2022, the IDPC played a pivotal role in a total of thirty-nine (39) cross-border cases, marking a significant stride from the preceding year's twenty-seven (27) cases. Of these cases, the IDPC assumed the role of a Lead Supervisory Authority in twenty-four (24) instances, representing a notable increase from

the twenty-one (21) cases in 2021. Concurrently, the IDPC acted as a Concerned Supervisory Authority in fifteen (15) cross-border cases, with a slight increase from 6 cases in 2021.

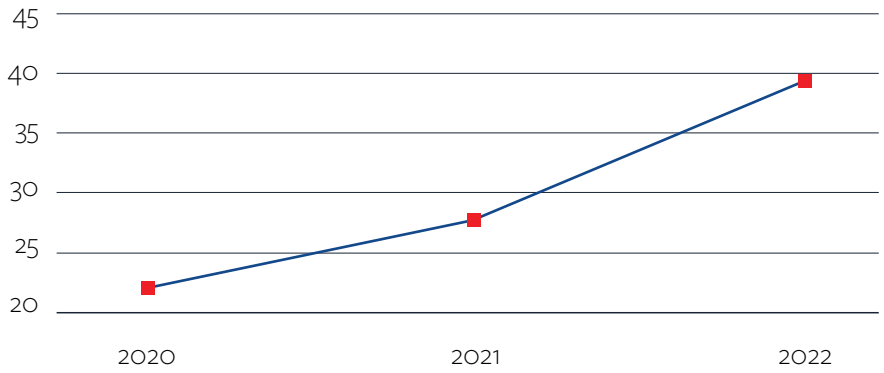
Within the ambit of our investigations, significant progress has been made, with fourteen (14) cases reaching completion, while scrutiny continues in twenty-five (25) ongoing investigations.

IMI Cases 2022



Additionally, our caseload has been steadily rising since 2020, starting with twenty-two (22) cases and increasing to twenty-seven (27) in 2021 and reaching thirty-nine (39) in 2022.

Comparison 2020-2022

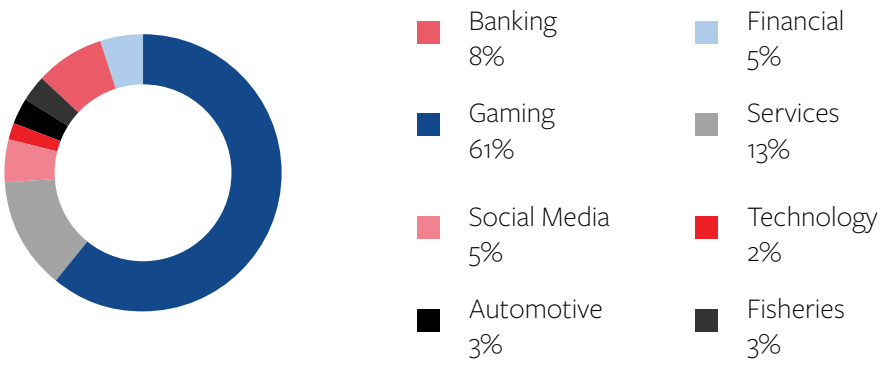


The sectoral distribution of controllers under investigation reveals a predominant focus on the online gaming industry, with twenty-four (24) cases emanating from organisations having their main establishment registered in Malta.

Sector of the Controller

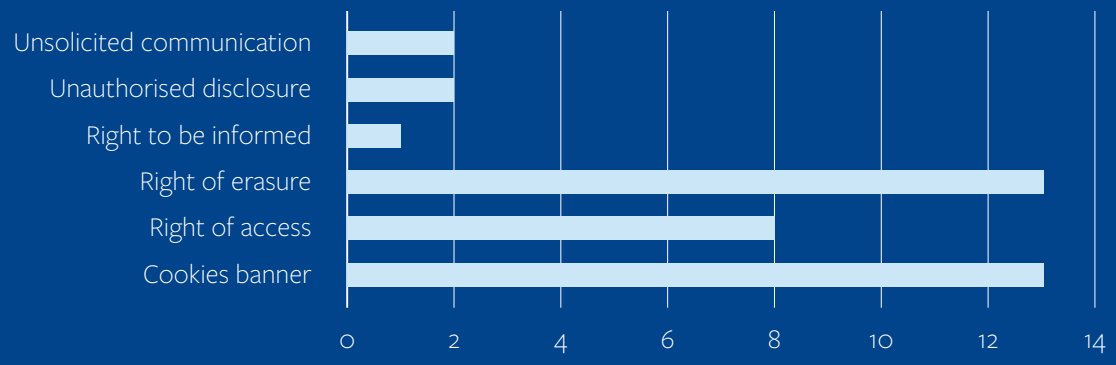
Banking	3
Financial	2
Gaming	24
Services	5
Social Media	2
Technology	1
Automotive	1
Fisheries	1
Total	**39**

Sector of the Controller



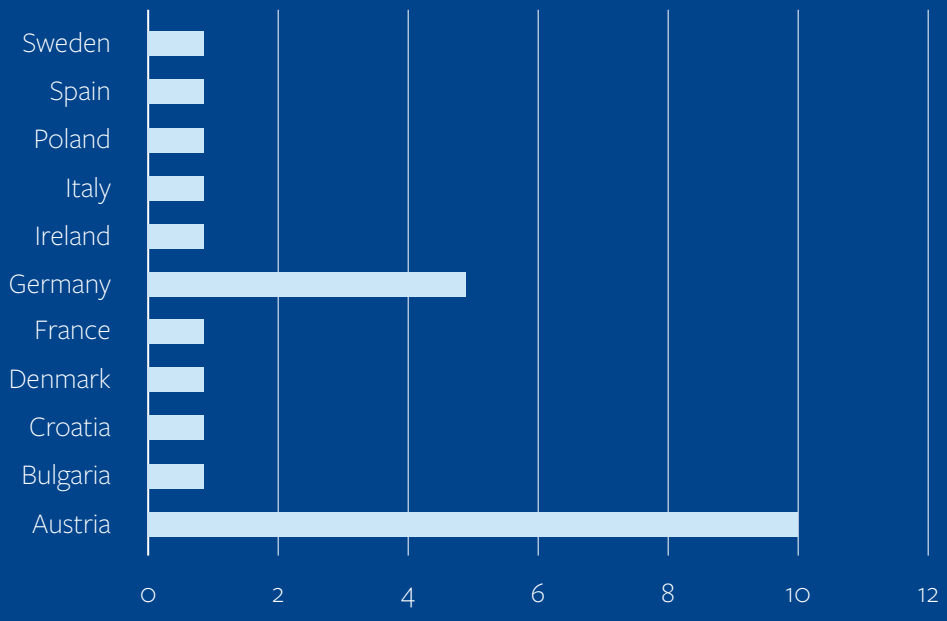
In delving into the nature of our investigations, a salient pattern emerges, with the exercise of data protection rights, notably the right of erasure, occupying a prominent position. Additionally, concerns regarding unsolicited marketing and compliance with cookie consent mechanisms have surfaced recurrently.

Cases by Nature



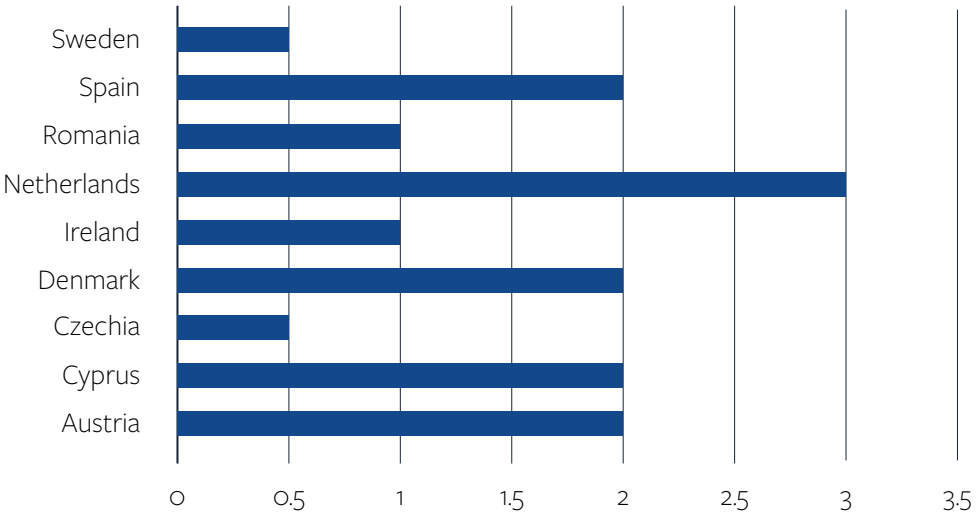
The chart below illustrates the number of countries from which IDPC has received complaints, designating it as the Lead Supervisory Authority. It is evident that Austria has contributed the highest number of complaints to IDPC. This trend may be attributed to Austria's current legal framework regarding gambling.

Country initiating complaint (LSA)



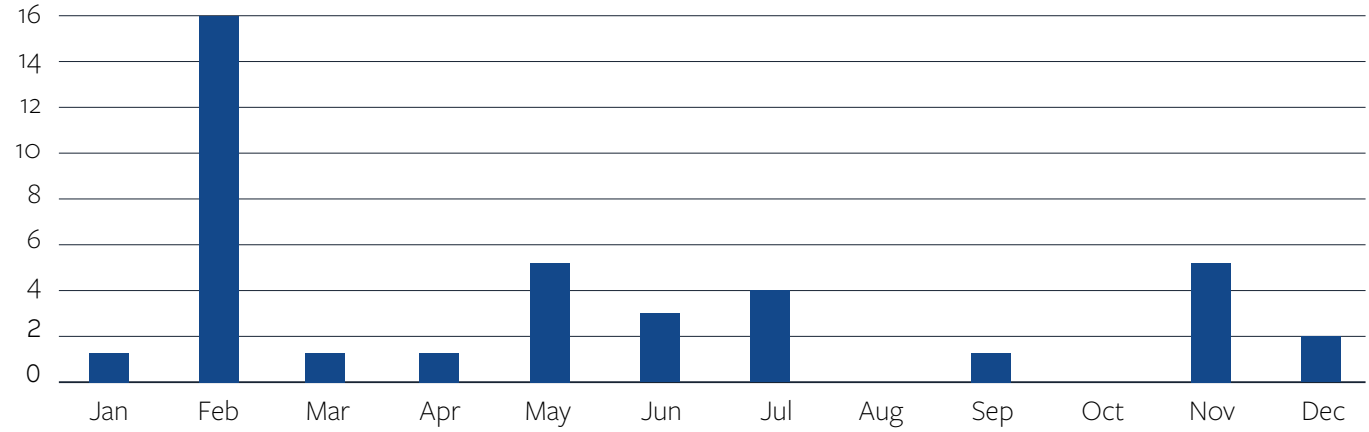
On the other hand, the graph below presents a list of countries to which IDPC has sent a complaint and was thus acting as a Concerned Supervisory Authority.

IDPC initiating complaint to country (CSA)



The graph below delineates the monthly distribution of cross-border complaints handled by IDPC throughout 2022. February emerges as the month with the highest caseload, conversely, August and October register no recorded cases.

Cases reported by month

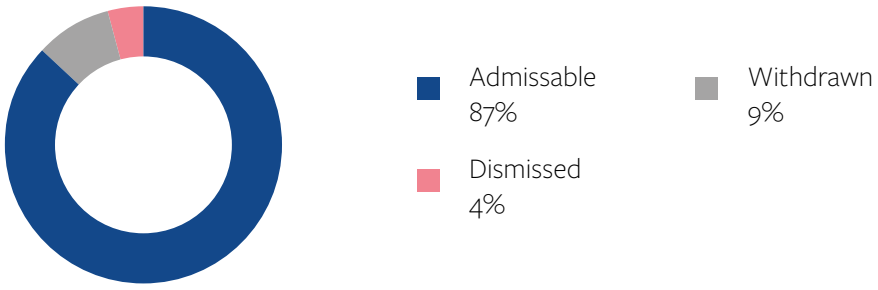


5.3 Personal data breaches

A personal data breach is one that affects the confidentiality, integrity or availability of personal data. Accidental deletion or ransomware attacks of personal data are also caught in this definition. Personal data breaches include incidents that are the result of both accidents (such as sending an email to the wrong recipient) as well as deliberate acts (such as phishing attacks to gain access to customer data). In terms of the GDPR if the security breach constitutes a risk to the rights and freedoms of natural persons, the supervisory authority must be notified within a maximum period of 72 hours of becoming aware of same. If the risk is classified as high risk, this must be communicated to those affected, without undue delay.

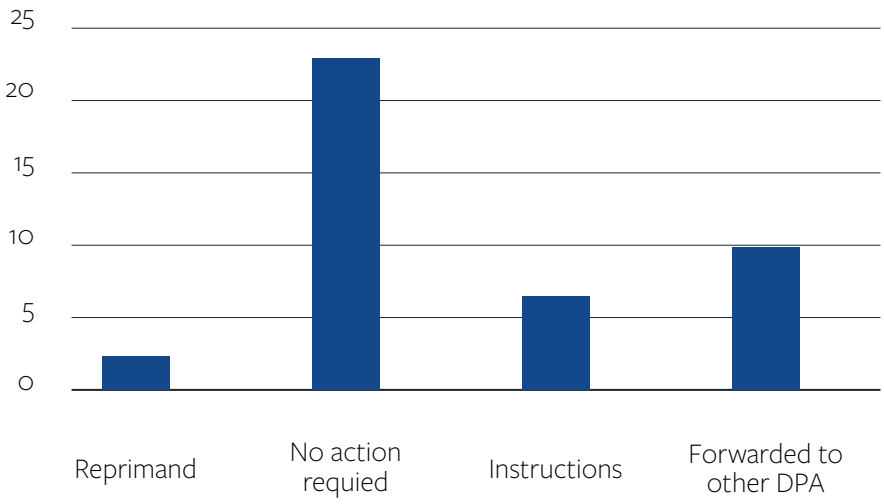
During the year under review, the IDPC received a total of fifty-nine (59) personal data breaches which is considerably less than the hundred (100) personal data breaches notified in 2021. Out of these fifty-nine (59) notifications, forty-seven (47) were investigated whilst the other twelve (12) were pending investigation. In terms of the below table, out of the forty-seven (47) personal data breach notifications, four (4) were withdrawn and two (2) were dismissed.

Nature of closed investigation



In terms of the below table, after the conclusion of the remaining forty-one (41) personal data breach notifications, the IDPC forwarded ten (10) to other supervisory authorities, issued instructions for another six (6), a reprimand for another two (2) and concluded that no action was required in respect of the remaining twenty-three (23) cases.

Actions identified by the IDPC on Admissible Cases

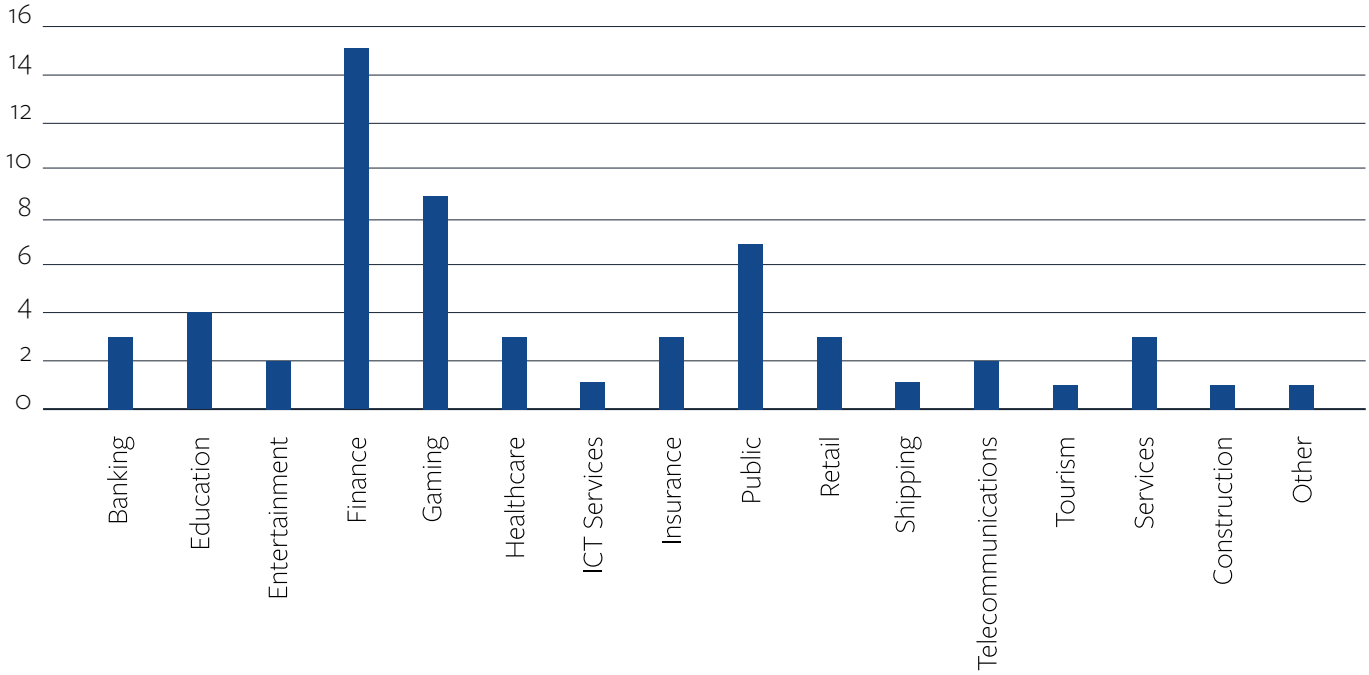


As per the table below the most frequent cause of personal data protection breach notified to the IDPC arose as a result of hacking and the second most frequent cause arose a result of personal data being sent out to the wrong recipient.

Subject	Closed	Pending	Total
Data of wrong data subject shown	2	1	3
Device lost or stolen or left in insecure location	1		1
External Malicious	2		2
External non malicious	1		1
Hacking	13	1	14
Incorrect disposal of data	1		1
Internal non malicious	1		1
Malware	6	1	7
Other	1		1
Paper lost or stolen or left in insecure location	2		2
Personal data sent to wrong recipient	8	1	9
Phishing	1	4	5
Disclosure of Personal Data	5	2	7
Unintended publication	3	2	5
Total	**47**	**12**	**59**

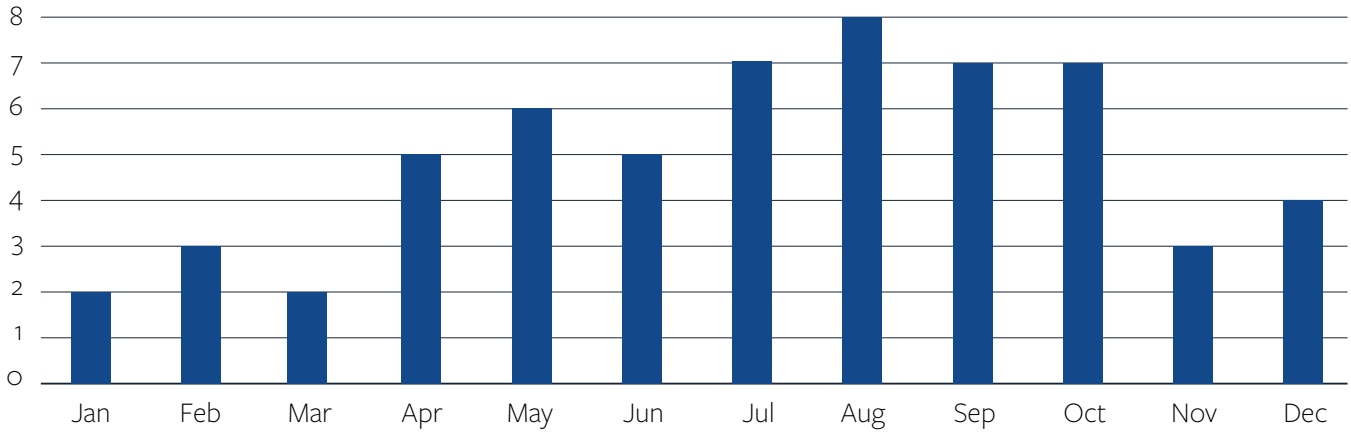
Out of the total personal data breach notifications received in the year under review, the sector most affected by data breaches is that of financial institutions followed by the gaming industry and then the public sector.

Reported Data Breach by Sector



As a concluding remark, the below graph represents the number of personal data breaches reported by month during the year under review.

Report by Month - 2022



6 SELECTED KEY DECISIONS

6.1 Personal Data Breaches

6.1.1 IT Company unlawfully processed personal data revealing political opinions

On the 14th January 2022, the IDPC issued a decision in relation to a personal data breach notified by an IT company. The IDPC became aware of the personal data breach after the media reported that a security vulnerability of a server pertaining to the IT company led to the exposure of over 335,000 personal records of voters in Malta. Subsequently, the company notified the personal data breach to the IDPC pursuant to article 33(1) of the GDPR.

The database contained the following data pertaining to 337,384 data subjects: (i) name and surname; (ii) identity card number; (iii) postal address: (iv) date of birth; (v) data subject's ballot box number; (vi) voting document number; (vii) district; (viii) phone number; (ix) sex and (x) numerical identifier from 1 to 4. The investigation revealed that the numerical identifier, combined with the other data, particularly the voting number and the ballot box number, is referring to the political opinions of the affected data subjects.

Following a thorough technical and legal analysis of the case, in the context of which, the IDPC duly assessed the evidence gathered during the course of investigation, it was established that the controller was not only storing the database on its servers in an unlawful manner, but it was also using this database as a template for various software projects developed for different clients. The IDPC decided that the controller infringed article 6(1), 9(1) and (2), 14 and 5(1)(f) of the Regulation.

The IDPC further concluded that the controller failed to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, which led to the incident to materialise. Additionally, the IDPC established that the controller failed to notify the personal data breach to this office within the deadline stipulated by law and to communicate the breach to the affected data subjects.

The IDPC considered the gravity and nature of the infringements, the fact that the controller is a microenterprise and its annual turnover, and consequently, imposed an effective, proportionate, and dissuasive administrative fine of sixty-five thousand euro (€65,000.00). Further to that, the IDPC ordered the controller to erase the personal data which were unlawfully processed.

The controller appealed the decision.

6.1.2 Gaming Company failed to implement the appropriate security measures which led to the exfiltration of its data pertaining to two million four hundred forty-six thousand, five hundred and twelve (2,446,512) data subjects

On the 4th October 2022, the IDPC issued a decision in relation to a personal data breach notified by a gaming company after it suffered a hacking attack which led to the access of personal data pertaining to two million, four hundred forty-six thousand, five hundred and twelve (2,446,512) data subjects.

The personal data breach involved cross-border processing of personal data which took place in the context of the activities of the main establishment of the controller, and which substantially affected data subjects in more than one Member State. The attacker managed to extract 3GB of customers' data.

The attack was initiated by the hacker when he managed to successfully exploit a chat functionality which was used by the customer support agents to provide support to its customers. By using the chat functionality, the attacker forwarded a malicious file to one of the customer support agents, and when it was executed by the agent, it downloaded and run a remote access trojan which was subsequently launched on the virtual machine being used by the agent.

The investigation conducted by the IDPC established that there were multiple failures by the controller, specifically, that it disregarded to assess the risk of varying likelihood and severity for the rights and freedoms of natural persons and consequently, to put in place appropriate technical and organisational measures to ensure a level of security appropriate to the risk in respect of the processing of personal data.

The IDPC decided that the controller infringed article 32(1) and article 32(2) of the GDPR and imposed an administrative fine of two hundred and fifty thousand euro (€250,000).

The controller appealed the decision.

6.2 Ex-officio investigation

6.2.1 Ex-officio investigation in relation to personal data which were left lying around in an abandoned hospital

The IDPC became aware of a video posted by a Youtuber who travels around the world to explore abandoned urban places. The video showed vandalised operating theatres, shattered medical equipment and thousands of medical records lying around in an abandoned hospital. The Youtuber flipped through files that still contained patients' data. The media further reported that the abandoned hospital became a haven for daredevils and vandals, who seem to have been breaking and entering repeatedly and smashing the place up.

The IDPC proceeded to initiate an ex-officio investigation after taking into consideration the gravity of the case, the nature of the personal data processed, the risks to the rights and freedoms of the data subjects, and the number of affected data subjects, and, on the 25th May 2022, the IDPC ordered the hospital to destroy all the personal data pursuant to article 58(2)(g) of the Regulation within ten (10) days.

The controller complied with the order.

6.3 Data Protection Complaints

6.3.1 Unauthorised access to, and disclosure of patient data to a third party

On the 31st January 2022, the IDPC issued a decision after it received a complaint from a data subject who alleged that an unauthorised third party accessed and disclosed medical data to her former partner.

From the evidence gathered during the course of the investigation, in particular, the audit trails, the Commissioner established that the employee accessed the medical data of the complainant on two instances. The controller failed to demonstrate that access to the data of the complainant was reasonably necessary for the purposes of providing or facilitating the provision of health care or for other related purpose. In fact, the controller confirmed that the employee accessed the personal data of the complainant for purely personal reasons which were certainly not related to the provision of health care.

The investigation revealed that the employee in question did not receive any training on data protection legislation despite being responsible for the handling of special categories of personal data as part of her day-to-day duties. In addition, the IDPC noted that the controller did not have in place any internal policies and processes to implement relevant data protection requirements for the particular processing operations carried out by the controller.

Accordingly, the IDPC decided that the controller infringed article 24(2), article 32(1)(b) and article 32(4) of the GDPR. The IDPC issued an administrative fine of two thousand five-hundred euro (€2,500) pursuant to article 21 of the Data Protection Act (Cap. 586 of the Laws of Malta). The IDPC also ordered the controller: (i) to provide training on data protection during the induction period for new employees and periodically to all the members of staff handling personal data; (ii) to implement procedures that are necessary to formalise and clarify practices to detect, prevent and reduce the risk of unauthorised access to personal data by employees; and (iii) to have in place confidentiality agreements.

The controller complied with the decision.

6.3.2 Processing of personal data when dispensing over-the counter non-prescription medication

On the 17th May 2022, the IDPC issued a decision after it received a complaint from a data subject alleging that a pharmacy is gathering and processing personal data, including special categories of personal data, through a completed form while dispensing over-the-counter, non-prescription medication, without valid legal justification and without obtaining the consent of the data subject.

In response, the IDPC requested the submissions of the controller on this matter, specifically asking for clarification on the legal basis for processing health-related data and to clarify who intended to process or further process any copies of the completed form. The controller stated that the data requested by the dispensing pharmacist adheres to the guidelines of the Malta Medicines Authority and that the forms are processed by the managing pharmacist.

Upon examination of the aforementioned guidelines, the IDPC determined that the pharmacist, acting in the patient's best interest, could only ensure the safety and appropriateness of the medication through a consultation process with the patient. This consultation necessitates the processing of certain health-related information, obtained through the collection of personal data contained in the dispensing record form.

After evaluating the type of data processed, the processing context, and its impact on the data subjects, the IDPC concluded that the controller's processing activities satisfied the conditions outlined in article 6(1)(f) and 9(2)(h) of the GDPR. However, the IDPC found an infringement of article 13 of the GDPR when it failed to provide the data subject with information concerning the processing of personal data at the time of the collection. As a result, pursuant to article 58(2)(d) of the GDPR. the IDPC ordered the controller to bring the processing operation into compliance with the provisions of the GDPR by adopting a data protection policy that contains all the requirements set forth in article 13 of the GDPR, including the storage period, and which shall be made available to all the data subjects at the time of collection of their personal data.

The controller complied with the decision.

FREEDOM OF INFORMATION

In 2022, the total number of requests received by public authorities from applicants exercising their right to access information under the Freedom of Information Act increased compared to the previous year. Specifically, in 2021, a total of five hundred and sixty-one (561) freedom of information requests were submitted, whereas in 2022, there were seven hundred and fifty-six (756) freedom of information requests. The average processing time for requests remained consistent at twenty-two (22) days throughout the year.

In 2022, the total number of accepted freedom of information requests amounted to three hundred and two (302), while three hundred and fifty (350) requests were rejected. These figures encompass cases carried over from 2021.

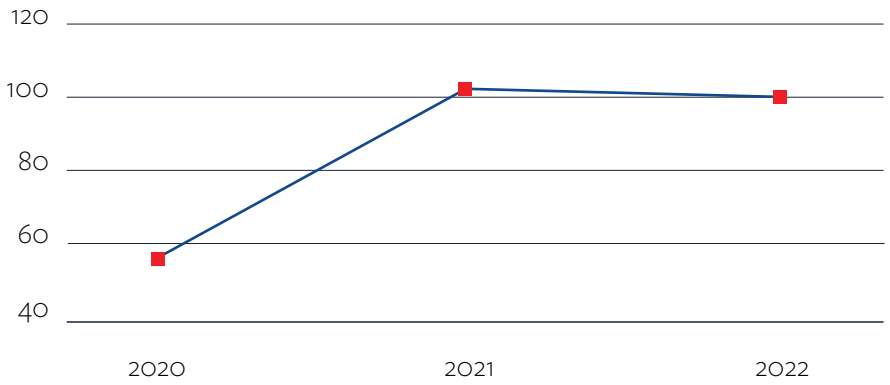
.

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

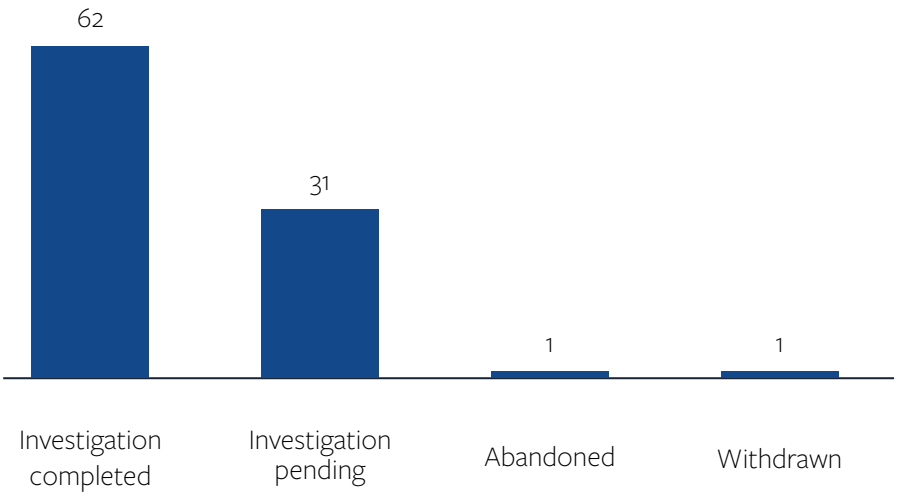
Reason for Requests refused	Total
Document requested is excluded from the scope of the Freedom of Information Act by virtue of Article 5	43
Document is withheld in terms of Part V or Part VI of the Act	81
The document requested is publicly available or will be published within three months.	35
The document requested cannot be found.	0
Resources required to identify, locate, or collate the document or documents would substantially and unreasonably divert the resources of the authority for its operations.	3
Resources required to examine the document or consult any person or body in relation to its possible disclosure would substantially and unreasonably divert the resources of the authority from its operations.	0
Resources required to make a copy, or an edited copy, of a document would substantially and unreasonably divert the resources of the Public Authority from its operations.	2
The document requested is not held by the Public Authority, or connected more closely with the functions of, another public authority.	71
The request is considered frivolous, trivial or vexatious.	0
The information relating to a decision or recommendation, requested pursuant to article 20 of the Act is being withheld in terms of Part V or VI of the said Act.	0
Other reasons	115
Total	**350**

In 2021, the IDPC received a total of hundred (100) applications under the Freedom of Information Act, of which ninety-five (95) were deemed admissible, and five (5) were found to be inadmissible.

Comparison



Outcome of admissable applications

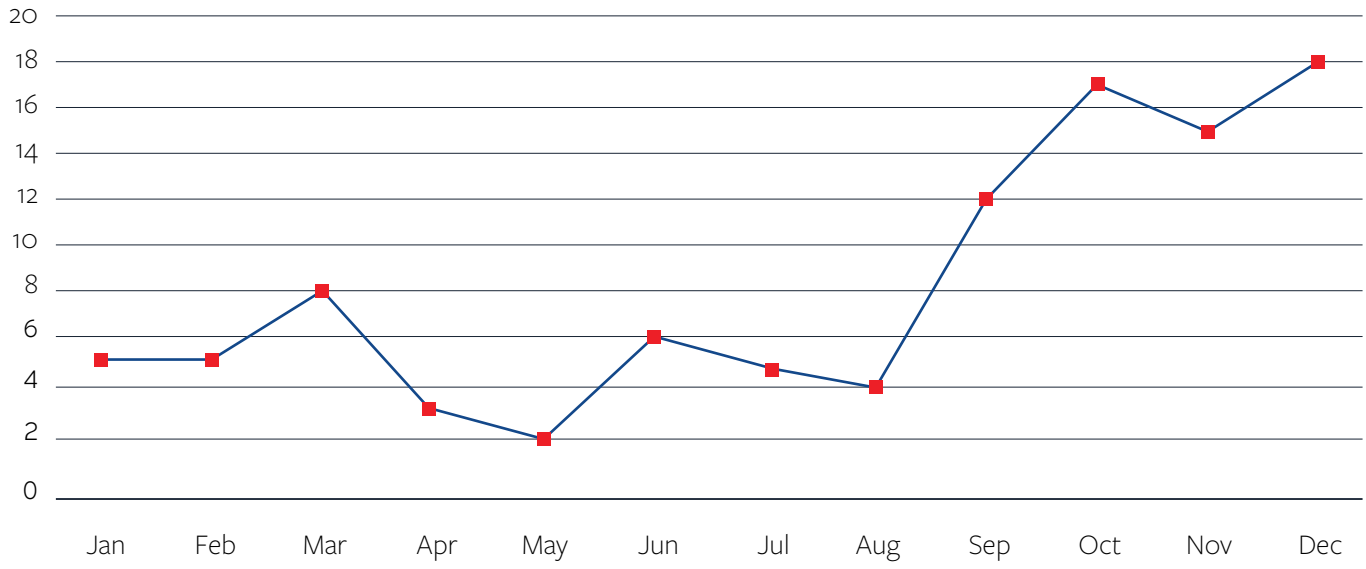


Appeals from the outcome of the investigation by the IDPC

Decision	No Appeal	Appeal	Total
Amicable Settlement	2	0	2
Decision Notice	2	1	3
Enforcement Notice	15	0	15
Information Notice	25	1	26
Information Notice & Amicable Settlement	5	1	6
Information Notice & Enforcement Notice	2	0	2
Instructions adhered to	8	0	8
Total	**59**	**3**	**62**

The graph below depicts the monthly distribution of freedom of information applications, with December having the highest number of applications, followed by October.

FOI applications by Month



8

APPENDIX 1:
FINANCIAL STATEMENTS

Office of the Information and Data Protection Commissioner

Annual Report and Financial Statements

For the Year Ended 31 December 2022

Office of the Information and Data Protection Commissioner

For the Year Ended 31 December 2022

Contents

Office of the Information and Data Protection Commissioner

Commissioner's Report

For the Year Ended 31 December 2022

The Commissioner presents this report and the audited financial statements of the Office of the Information and Data Protection Commissioner (hereunder referred to as "the Office") for the year ended 31 December 2022.

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 also to administer the provisions of the Freedom of Information Act.

Results

During the year, the Office registered a surplus of €27,024 (2021: a surplus of €28,769) before taking into account the result from the collection of notification fees. The Office received Government subvention amounting to €680,000 in 2022, representing an increase of 10% when compared to 2021. Total administrative expenditure amounted to €650,106, resulting in an increase of 6% when compared to 2021. As from 1 January 2016, the Government and the Office have agreed that notification fees received by the Office, 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 Office. In 2022, the Office did not collect any notification fees (2021: Nil).

The results for the year are set out on in the Statement of Comprehensive Income on page 5.

Going Concern

The financial statements have been prepared on the going concern basis which assumes that the Office 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 Office to meet its commitments as and when they fall due.

Events after the balance sheet date and future developments

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

Commissioner

The present Commissioner who held office during the year was:

Mr. Ian Deguara

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 Office 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 Office 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 Office 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 14 July 2023 and signed by:

_____

Mr. Ian Deguara
Commissioner

Registered Address:
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 19 which comprise the statement of financial position as at 31 December 2022, the statement of comprehensive income, statement of changes in equity and statement of cash flows for the year then ended, and notes to the financial statements, including a summary of significant accounting policies.

In our opinion, the accompanying financial statements give a true and fair view of the financial position of the Office as at 31 December 2022, 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 Office 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 Office 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 Office'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 Office 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 Office'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 Office'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 Office to cease to continue as a going concern.

- Evaluate the overall presentation, structure and content of the financial statements, including the disclosures, and whether the financial statements represent the underlying transactions and events in a manner that achieves fair presentation.

We 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, Level 3, Mannarino Road
Birkirkara BKR 9080
Malta

14 July 2023

Office of the Information and Data Protection Commissioner

Statement of Comprehensive Income

For the Year Ended 31 December 2022

	Note	2022	2021
		€	€
Government subvention		680,000	620,000
Administrative expenses		(650,106)	(614,302)
Finance costs		(9,954)	(5,229)
Other income		7,084	28,300
Surplus for the year	3.	**27,024**	**28,769**

The notes on pages 9 to 19 form an integral part of these financial statements.

Office of the Information and Data Protection Commissioner

Statement of Financial Position

As at 31 December 2022

	Note	2022 €	2021 €
ASSETS			
Non-current assets			
Property, plant and equipment	6.	325,841	369,139
Current assets			
Trade and other receivables	7.	1,541	10,672
Cash and cash equivalents	8.	216,223	147,073
Total current assets		217,764	157,745
TOTAL ASSETS		543,605	526,884
EQUITY AND LIABILITIES			
Equity			
Retained Funds		149,355	122,331
Liabilities			
Non-current liabilities			
Lease liabilities	9.	289,367	312,702
Current liabilities			
Lease liabilities	9.	23,335	22,646
Trade and other payables	10.	81,548	69,205
Total current liabilities		104,883	91,851
TOTAL EQUITY AND LIABILITIES		543,605	526,884

The notes on pages 9 to 19 form an integral part of these financial statements.

These financial statements on pages 5 to 19 were approved by the Office of the Information and Data Protection Commissioner on 14 July 2023 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 2022

	Retained Funds	Total Equity
	€	€
Balance as at 01 January 2022	122,331	122,331
Surplus for the year - total comprehensive income	27,024	27,024
Balance as at 31 December 2022	149,355	149,355

	Retained Funds	Total Equity
	€	€
Balance as at 01 January 2021	93,562	93,562
Surplus for the year - total comprehensive income	28,769	28,769
Balance as at 31 December 2021	122,331	122,331

The notes on pages 9 to 19 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 2022

	Note	2022 €	2021 €
Cash from operating activities:			
Surplus from operations		27,024	28,769
Interest expense		9,954	5,229
Depreciation		43,298	42,848
Profit from operations		80,276	76,846
Movement in trade and other receivables		9,132	(6,763)
Movement in trade and other payables		12,342	(26,770)
Net cash flows from operating activities		101,750	43,313
Cash flows from investing activities:			
Payments for property, plant and equipment		-	(3,198)
Net cash flows from/(used in) investing activities		-	(3,198)
Cash flows from financing activities:			
Repayment of finance lease liabilities		(32,600)	(32,600)
Net cash from cash and cash equivalents		69,150	7,515
Cash and cash equivalents at beginning of year		147,073	139,558
Cash and cash equivalents at end of year	8.	216,223	147,073

The notes on pages 9 to 19 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 Office'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 Office has applied new and amended IFRS Standards issued by the International Accounting Standards Board (IASB) and adopted by the EU that are mandatorily effective in the EU for an accounting period that begins on or after 1 January 2021. The adoption of new and amended standards did not have a material impact on the Council’s financial statements.

- Amendment to IFRS 16 Leases: COVID-19-Related Rent Concessions beyond 30 June 2021 (applicable for annual periods beginning on or after 1 April 2022)
- Amendments to IAS 16 Property, Plant and Equipment: Proceeds before Intended Use (applicable for annual periods beginning on or after 1 January 2022)
- Amendments to IAS 37 Provisions, Contingent Liabilities and Contingent Assets: Onerous Contracts — Cost of Fulfilling a Contract (applicable for annual periods beginning on or after 1 January 2022)
- Amendments to IFRS 3 Business Combinations: Reference to the Conceptual Framework (applicable for annual periods beginning on or after 1 January 2022)
- Annual Improvements to IFRS Standards 2018–2020 (applicable for annual periods beginning on or after 1 January 2022)

The Office has assessed the effects of these standards and interpretations and is of the opinion that these did not have a material impact on these financial statements.

1. Basis of Preparation (Continued)

e. Changes in accounting policies and disclosures (Continued)

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

Up to date of approval of these financial statements, certain new standards, amendments and interpretations to existing standards have been published but which are not yet effective for the current reporting year and which the Office has not early adopted, but plans to adopt upon their effective date. The Office is still assessing the effect of these changes on the financial statements. The new and amended standards are as follows:

- IFRS 17 Insurance Contracts (applicable for annual periods beginning on or after 1 January 2023)
- Amendments to IFRS 17 Insurance contracts: Initial Application of IFRS 17 and IFRS 9 – Comparative Information (applicable for annual periods beginning on or after 1 January 2023)
- Amendments to IAS 1 Presentation of Financial Statements: Classification of Liabilities as Current or Non-current and Non-current Liabilities with Covenants (applicable for annual periods beginning on or after 1 January 2024 or later, but not yet endorsed in the EU)
- Amendments to IAS 1 Presentation of Financial Statements and IFRS Practice Statement 2: Disclosure of Accounting Policies (applicable for annual periods beginning on or after 1 January 2023)
- Amendments to IAS 8 Accounting policies, Changes in Accounting Estimates and Errors: Definition of Accounting Estimates (applicable for annual periods beginning on or after 1 January 2023)
- Amendments to IAS 12 Income Taxes: Deferred Tax related to Assets and Liabilities arising from a Single Transaction (applicable for annual periods beginning on or after 1 January 2023)
- Amendments to IFRS 16 Leases: Lease Liability in a Sale and Leaseback (applicable for annual periods beginning on or after 1 January 2024, but not yet endorsed in the EU)

The Office is still assessing the effect of these changes on the financial statements.

f. Going concern

The financial statements have been prepared on the going concern basis which assumes that the Office 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 Office 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 Office 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.

2. Significant Accounting Policies (Continued)

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%
Computer software	25%
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 office's non-financial assets are reviewed at each reporting date to determine whether there is any indication of impairment. If such indication exists, then the asset's recoverable amount is estimated.

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

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

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

2. Significant Accounting Policies (Continued)

d. Financial instruments

i. Recognition and derecognition

Financial assets and financial liabilities are recognised when the Office 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 Office 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 Office'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 Office's first identifying a credit loss event. Instead the Office 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 Office's financial liabilities were not impacted by the adoption of IFRS 9. However, for completeness, the accounting policy is disclosed below.

The Office'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 Office 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).

Iinterest-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 Office 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. Bank overdrafts are presented as current liabilities in the statement of financial position.

g. Provisions and contingent liabilities

A provision is recognised when, as a result of a past event, the Office has a present obligation that can be estimated reliably and it is probable that the Office 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 Office'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 Office 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 currency translation

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 Entity contributes towards the state pension in accordance with local legislation. The only obligation of the Entity 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 Office'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. Liquidity risk

The Office 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.

ii. Fair values

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

iii. Capital risk management

The Office's objectives when managing capital are to safeguard its ability to continue as a going concern. The capital structure of the Office 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:

	2022	2021
	€	€
Auditors remuneration	2,448	2,065
Depreciation expense	43,298	42,848
Total	45,746	44,913

4. Taxation

The Commissioner as per previous practice, considers the Office as tax exempt and did not provide for tax at 35% in the financial statements. A tax exemption on the surplus, in terms of Article 12(2) of the Income Tax Act, has been requested from the Ministry of Finance.

5. Wages and Salaries

a. Wages and salaries

Payroll costs for the year comprise of the following:

	2022	2021
	€	€
Salaries and wages	466,284	443,651
Social security contributions	29,839	30,683
Total	496,123	474,334

b. Average number of employees

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

	2022	2021
	No.	No.
Commissioner	1	1
Directly employed by the Office	13	13
Total	14	14

6. Property, plant and equipment

	Right of use assets	Furniture and fixtures	Motor vehicles	Office equipment	Computer software	Air conditioners	Total
	€	€	€	€	€	€	€
Cost							
Opening balance	362,719	67,570	17,400	68,931	25,038	4,178	545,836
Balance at 31 December 2022	362,719	67,570	17,400	68,931	25,038	4,178	545,836
Depreciation							
Opening balance	(32,974)	(47,151)	(17,400)	(57,344)	(19,055)	(2,773)	(176,697)
Depreciation	(32,974)	(2,818)	-	(3,512)	(3,003)	(991)	(43,298)
Balance at 31 December 2022	(65,948)	(49,969)	(17,400)	(60,856)	(22,058)	(3,764)	(219,995)
Net Book Value							
At 31 December 2021	329,745	20,419	-	11,587	5,983	1,405	369,139
At 31 December 2022	296,771	17,601	-	8,075	2,980	414	325,841

a. Right-of-use assets

Right-of-use assets represents 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

	2022	2021
	€	€
Notification fee receivables	222,374	222,374
Provision for doubtful debts for notification fees	(222,374)	(222,374)
Prepayments	1,541	1,668
Other receivable	-	9,004
Total	1,541	10,672

8. Cash and cash equivalents

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

	2022	2021
	€	€
Cash on hand	1,015	511
Bank balances	215,208	146,562
Total cash and cash equivalents in the statement of cash flows	216,223	147,073

9. Lease liabilities

a. Amounts recognised in the statement of financial position

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

	2022	2021
	€	€
Right-of-use assets		
Buildings	296,771	329,745
Lease liabilities		
Current	23,335	22,646
Non-current	289,367	312,702
Total	312,702	335,348

The maturity of lease commitments is analysed as follows:

	2022	2021
	€	€
Less than one year	23,335	22,646
Between one and five years	112,700	136,035
More than five years	176,667	176,667
	312,702	335,348

b. Amounts recognised in the statement of comprehensive income

The statement of comprehensive income shows the following amounts relating to leases:

	2022	2021
	€	€
Amortisation of right-of-use assets	32,975	32,974
Interest expense	9,954	5,229

The total cash outflow of the Office for leases during the year ended 31 December 2022 is €32,600.

10. Trade and other payables

	2022	2021
	€	€
Amount payable to related parties (Note 11.)	53,547	31,047
Accruals	28,001	38,158
Total	81,548	69,205

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

11. Related Party Transactions

The Office of the Information and Data Protection Commissioner is an independent Office and reports to Parliament on an annual basis. The Commissioner is appointed by the Government of Malta. In terms of the Freedom of Information Act, the Commissioner will not seek or receive instructions from public authorities or from any other institution or authority.

Year end balances payable to related parties are disclosed in note 10.

Office of the Information and Data Protection Commissioner

For the Year Ended 31 December 2022

Schedules

Schedule of Administrative Expenses

	2022	2021
	€	€
Wages and Salaries	496,123	474,334
Accountancy Fees	13,011	13,631
Auditors remuneration	2,448	2,065
Advertising Fees	531	3,361
Cleaning of premises	3,452	3,149
Consumables	4,862	6,124
Water and Electricity Fees	2,151	2,313
Car Hire Expenses	4,989	13,258
Entertainment	149	-
Insurance	20	26
IT expenses	553	153
Fuel Expenses	6,034	3,351
Printing, Postage and Stationery Fees	3,309	3,621
Repairs and Maintenance Fees	19,462	18,670
Internet Subscription Fees	211	162
Telephone Fees	4,518	3,703
Travelling Fees	31,930	7,124
Parking Fees	3,501	4,503
Registration Fees	2,100	4,416
Hospitality Costs	429	1,928
General and Incidental Expenses	6,335	4,895
Bank charges	689	667
Depreciation and Amortisation	43,298	42,848
Total	650,105	614,302

Schedules do not form part of the audited financial statements.