idpc.
INFORMATION AND DATA PROTECTION COMMISSIONER

Annual Report **2020**


idpc.
INFORMATION AND DATA
PROTECTION COMMISSIONER

Contents

Foreword

This is my first annual report as Information and Data Protection Commissioner after taking over and continuing to build on the sterling work performed by my predecessor during his term in office. I can say that 2020 could be considered as a unique one. The outbreak of the pandemic, an unprecedented event, has radically changed a number of things around us, from the manner how we had to adjust our means to be able to communicate with each other, to having to find solutions to ensure that our children continue receiving their education, to effectively and safely providing a health care treatment to our patients and to pursue our resolve to proceed with our daily lives while at the same time adapting ourselves to this new reality.

This annual report compiles the results of our strenuous efforts in making sure that the protection of personal data and the right of information of individuals continue to be upheld unhindered during the health crisis. In so doing, we ensured to make ourselves available at all times to anyone seeking our expert advice, particularly on COVID-19 matters.

The current state of technology allows people to meet and interact online and do most of their work without leaving their homes. I believe these changes have come to stay and are likely to pose new challenges in terms of data protection and data security.

On a positive note, during this year, I have observed a significant increase in individuals' awareness of their data protection rights and an acceptable level of compliance by controllers and processors. I consider this as a demonstration that regulations are well understood and received by the public.

I would like to spend a word of appreciation to my staff, who with great dedication and professionality has shown flexibility in adapting to such unusual circumstances while preserving the expected level of public service.

Ian Deguara
Information and Data Protection Commissioner

1

2020 at a Glance

470
Data Protection Complaints

95
Data Breach Notifications

58
Freedom of Information Complaints

15
Full-time Members of Staff

€550K
Annual Budget

€45K
Administrative Fines

€200K +
In EU Funds for Data Protection Awareness and Help SMEs

795
Registered DPOs Private Sector

335
Registered DPOs Public Sector

2

Our Office

2.1

Our mission and vision

The IDPC is the independent supervisory authority responsible for monitoring the application of data protection law in Malta. Our mission is to ensure that the fundamental rights and freedoms of natural persons in relation to processing of personal data are protected, while facilitating the free flow of personal data within the European Union. The IDPC is also responsible for facilitating the right to access information held by public authorities to promote added transparency and accountability in government.

The IDPC believes that safeguarding a high level of personal data protection and ensuring that individuals also their right to freedom of information held by public authorities are essential components of a democratic, open and transparent society.

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 law;
- enforcing data protection rules by taking appropriate corrective action against controllers and processors which are found infringing the law;
- assisting SMEs in complying with the data protection law;
- taking initiatives to raise data protection awareness, also making use of dedicated EU funds to achieve this objective;
- contributing to the consistent application of the GDPR 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 operations public sector entities and bodies in conducting their operations.

2.3

The laws that we regulate

2.3.1 Data protection

The General Data Protection Regulation

Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, commonly referred to as the "General Data Protection Regulation" or "GDPR", entered into force on 24 May 2016 and started applying from 25 May 2018. The GDPR is an essential step to strengthen individuals' fundamental rights in the digital age and facilitate business by clarifying rules for companies and public bodies in the digital single market. The GDPR allows individuals to better control their personal data. It also modernises and unifies rules, allowing businesses to reduce red tape and to benefit from greater consumer trust. The GDPR also establishes a system of completely independent supervisory authorities in charge of monitoring and enforcing compliance, of which the IDPC form part. Arguably, the GDPR is the most comprehensive and significant component of the EU data protection law reform, along with the Law Enforcement Directive, which is also described here below.

The Data Protection Act and Subsidiary Legislation

On the 28th May 2018, Malta further implemented and specified the provisions of the GDPR by means of Act XX of 2018 of Parliament, the Data Protection Act, recorded under Chapter 586 of the Laws of

Malta. The new Data Protection Act repealed and replaced the former Data Protection Act (Chapter 440 of the Laws of Malta), which remained in force for nearly two decades and effectively shaped the central role of data protection in the Maltese jurisdiction, along with the functions of the IDPC.

The Data Protection Act also conforms to the principles of the Convention of the Council of Europe for the Protection of Individuals Regarding Automatic Processing of Personal Data, the first legally binding instrument recognising the international dimension of data protection by introducing measures to safeguard the rights of individuals against abuses in the collection and processing of their personal data, and to regulate the trans-frontier flow of personal data. The Republic of Malta ratified the Convention in 2003. Subsequently, the Convention was supplemented by a number of additional protocols, including the recent modernisation into the "Convention 108 +" of 2018.

By virtue of his powers, the Minister responsible for data protection has issued Legal Notices laying down further requirements in relation to certain specific aspects of data protection. These are being recompiled here below:

- Subsidiary Legislation 586.01: "Processing of Personal Data (Electronic Communications Sector) Regulations".

Refer to the "e-Privacy Directive" section below.

- Subsidiary Legislation 586.02: "Notification and Fees (Data Protection Act) Regulations".

These regulations revoked the obligation to notify all processing operations to the IDPC, and to pay the corresponding fee.

- Subsidiary Legislation 586.03: "Third Country (Data Protection Act) Regulations".

These regulations revoked the rules concerning transfers of personal data to countries which are not Member States of the European Union priorly in force. The discipline concerning transfers of personal data to third countries or international organisations is currently found in Chapter V of the GDPR.

- Subsidiary Legislation 586.04: "Processing of Personal Data (Protection of Minors) Regulations".

These regulations give any teacher, member of a school administration person acting in loco parentis or in a professional capacity in relation to a minor, the capacity to collect and in any other way process personal data in relation to that minor without the need to request the parents' consent, as long as the processing is in the best interest of the minor. The provisions of this Act are without prejudice to the obligation to consult and, or obtain prior authorisation by the IDPC, as the case may be.

- Subsidiary Legislation 586.05: "Transfer of Personal Data to Third Countries Order".

These regulations revoked the former Minister's order on transfers of personal data to certain third countries for specific purposes.

- Subsidiary Legislation 586.06: 'Processing of Personal Data for the Purposes of the General Elections Act and the Local Government Act Regulations'.

These regulations stipulate that personal data, including sensitive personal data, the processing of which is provided for in the General Elections Act (Chapter 354 of the Laws of Malta) and in the Local Government Act (Chapter 363 of the Laws of Malta), may be processed by any person entitled to process such data for the purpose of the implementation of the General Elections Act and the Local Government Act.

- Subsidiary Legislation 586.07: "Processing of Personal Data (Education Sector) Regulations".

These regulations set forth specific provisions applicable data processing operations carried out by controllers operating within the education sector.

- Subsidiary Legislation 586.08: "Data Protection (Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties) Regulations".

Refer to the "Law Enforcement Directive" section below.

- Subsidiary Legislation 586.09: "Restriction of the Data Protection (Obligations and Rights) Regulations".

Article 23 of the GDPR lists a number of requirements to be met in order for a measure restricting the rights of the data subjects and certain obligations of the controller to be lawfully relied upon. Restrictions must respect the essence of the fundamental rights and freedoms and must be a necessary and proportionate measure in a democratic society to safeguard certain primary conditions. Further to this, restrictions must be foreseeable and laid down by Union or Member State law.

One of these legislative measures is Subsidiary Legislation 586.09, which indicates the grounds based on which restrictions may apply, along with the necessary conditions and safeguards.

- Subsidiary Legislation 586.10: "Processing of Data concerning Health for Insurance Purposes Regulations".

These regulations reconcile the specific processing operations attached to the business of insurance and to insurance distribution activities, which may involve processing of data concerning health. In essence, processing personal data concerning health shall be deemed to be in the substantial public interest when such processing is necessary for the purpose of the business of insurance or insurance distribution activities, without prejudice to the implementation of suitable and specific measures designed to safeguard the fundamental rights and freedoms of data subjects.

- Subsidiary Legislation 586.11: "Processing of Child's Personal Data in Relation to the Offer of Information Society Services Regulations".

Information society services are services provided for remuneration, at the request of the recipient and at a distance during the connection of electronic devices by an electronic communication network. Taking into account the risks of processing personal data of children in providing them with information society services, article 8 of the GDPR provides that the processing of the personal data of a child in relation to the offer of information society services directly to the child shall be lawful where the child is at least 16 years old. The same provision stipulates that where the child is below the age of 16 years, the processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Article 8 of the GDPR foresees that Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years. Subsidiary Legislation 586.11 does so by lowering that age to 13 years.

The Law Enforcement Directive

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, also referred as Law Enforcement Directive, ensures the protection of personal data of individuals involved in criminal proceedings, be it as witnesses, victims or suspects.

The Law Enforcement Directive, which is also part of the EU data protection reform package, establishes a comprehensive framework to ensure a high level of data protection, while taking into account the specific nature of the police and criminal justice field. It contributes to increased trust and facilitates cooperation in the fight against crime in Europe by harmonising the protection of personal data by law enforcement authorities in EU Member States and Schengen countries.

Directives are binding legislative acts addressed to Member States setting out goals to be achieved in a consistent manner. Malta implemented the Law Enforcement Directive into Subsidiary Legislation 586.08, titled "Data Protection (Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties) Regulations". The Act specifies and implements the objectives of the Law Enforcement Directive into national law, taking into account the peculiarities of the Maltese police and criminal justice system, and designated the IDPC as the independent public authority established in Malta responsible for monitoring the application of the national implementation of the Law Enforcement Directive.

The e-Privacy Directive

Information is exchanged through public electronic communication services such as the internet, mobile and landline telephony and via their accompanying networks. These services and networks require specific rules and safeguards to ensure the users' right to privacy and confidentiality. These were introduced by Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, also known as "e-Privacy Directive". The e-Privacy Directive was a milestone in the regulation of data protection in the electronic communications sector by setting out rules to ensure security in the processing of personal data, the notification of personal data breaches, and confidentiality of communications. As a general rule, it also bans unsolicited communications where the user has not given their consent. Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 intervened to bring amendments to the e-Privacy Directive as part of the EU's telecoms reform package.

The e-Privacy Directive and its subsequent amendments were enacted into Maltese law by means of Subsidiary Legislation 586.01, titled "Processing of Personal Data (Electronic Communications Sector)". The IDPC has a primary role in these regulations, and it is assigned with a wide range of powers to verify compliance thereof by providers of publicly available electronic communications services.

2.3.2 Re-Use of Public Sector Information

Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and reuse of public-sector information lays down the legal framework for the reuse by persons or legal entities of documents held by public-sector bodies or public undertakings such as geographical, land registry, statistical or legal information and of publicly funded research data. The core principle of the Directive is that public and publicly funded data should be reusable for commercial or non-commercial purposes. In doing so, the Directive aims at boosting the socioeconomic potential of public-sector information by promoting competition and transparency in the information market, and it is part of a package of measures designed to reinforce the EU's data economy, including the development of artificial intelligence.

The provisions of the Directive were implemented into Chapter 546 of the Laws of Malta, titled "Re-Use of Public Sector Information Act", which also appointed the IDPC as the regulatory authority responsible for the monitoring of the implementation of the Act.

2.3.3 Freedom of Information

As part of its regulatory functions, the IDPC is entrusted with promoting the observance by relevant public authorities of the requirements of the Freedom of Information Act, recorded as Chapter 496 of the Laws of Malta. The Freedom of Information Act gives people a general right of access to information held by most public authorities. Aimed at promoting a culture of openness and accountability across the public sector, it enables a better understanding of how public authorities carry out their duties. Under the Freedom of Information Act, eligible persons are entitled to request documents held by a public authority without giving reason or the need to justify their request. Eligible persons also have a right to remedy in relation to such requests, which can be exercised by lodging a complaint with the IDPC. The IDPC recognises that the Freedom of Information Act is a is a significant piece of legislation which merits all necessary attention, from a regulatory viewpoint, being an integral part of a democratic society built on rule of law.

2.3.4 Freedom of Access to information on the Environment

Directive 2003/4/EC of the European Parliament and of the Council on public access to environmental information was introduced with the objective of adapting the laws of the Members States to the 1998 Aarhus Convention on access to information, public participation and access to justice in environmental matters. The Directive requires that Member States guarantee that the public has access to environmental information held by, or for, public authorities, both upon request and through active dissemination. The Directive also sets out the basic terms, conditions and practical arrangements that a member of the public must respect when granted access to the requested environmental information.

In Malta, the Directive was enacted by Subsidiary Legislation 549.39, titled "Freedom of Access to Information on the Environment Regulations". The purpose of these regulations is, apart from the transposition of the Directive, to guarantee the right of access to environmental information held by or for public authorities and to set out the basic terms and conditions of, and practical arrangements for, its exercise and to ensure that, as a matter of course, environmental information is progressively made available and disseminated to the public in order to achieve the widest possible systematic availability and dissemination to the public of environmental information.

The IDPC is competent to receive applications for decisions on infringements of these regulations by any person who has previously made a request to be provided with environmental information by a competent authority and is dissatisfied with the response obtained.

2.4 Staff compliment and budget

The Office of the Commissioner has a staff complement of 15 employees, who are distributed in three main units: legal, technical and administrative. Notwithstanding this separation, IDPC's employees have developed a degree of versatility in handling both data protection and freedom of information cases with a high level of competence and professionalism. It often occurs that the legal and the technical team work closely, especially in cases which both legal and technical expertise is required, such as personal data breaches.

The IDPC invests the necessary resources in training its staff to ensure that the members of the office remain abreast of the developments in data protection legislation, in particular in light of the rapid developments in technology.
Given the significant increase of the office's workload, which keeps rising steadily after the entry into force of the GDPR, the IDPC is planning to extend its workforce during the upcoming year.

The budget allocated by the Government for the year 2020 to cover the office's expenses totalled to an amount of EUR 550,000. A detailed analysis and breakdown of the expenses incurred by the IDPC during 2020 is included in the yearly financial statements annexed to this annual report. The revenue generated by this Office is periodically transferred to the line Ministry, and it accrues to the Government's consolidated fund.

3

Engagements

3.1

Activities and presentations

One of the functions of the IDPC is to promote public awareness and understanding of the risks, rules, safeguards, and rights in relation to data protection amongst controllers and processors of the one part, and data subjects of the other part. To achieve this objective, the IDPC took initiatives to promulgate such awareness for the benefit of the citizens and all other stakeholders.

The Commissioner and his staff participated in several events, conferences or seminars on data protection organised by organisations belonging to both public and private sector public sector and to the civil society. Amongst others, the addressees of the IDPC's interventions were legal professionals, ICT professionals, the Judiciary, engineers, accountants, SMEs, data protection officers, retailers, sole traders, trade unions, employers, academics, post-secondary students, hoteliers and security personnel at hotels, financial services professionals and online gaming professionals.

Due to the impediments brought by the pandemic, the number of physical meetings decreased. On the other hand, countless calls and online meetings were entertained by the IDPC to discuss data protection matters and to answer specific queries related to data protection.

Each year, in occasion of the data protection day, the Data Protection Unit organises a one-day seminar addressed to all Public Service and Public Sector data protection officers.

During the 2020 edition of the event, the following presentations were delivered:

- Data Pseudonymisation and Anonymisation Techniques;
- Common Issues: Implementing the GDPR;
- E-Privacy Regulation and Brexit;
- Statistical Information on Personal Data Breaches.

In addition to the above, the former Commissioner delivered a speech wherein he stressed the central role of data protection as a fundamental right and opined that the Data Protection Day is the result of a continued efforts and sincere cooperation between the competent authorities. He also drew the attendees' attention to the importance of making responsible choices as data subjects when entrusting controllers and processors with their personal data.

3.2

Data Protection Day

28 January is Data Protection Day. The date marks the anniversary of the Council of Europe's Convention 108 on the protection of personal information, the first legally binding international law in the field of data protection being celebrated every year by the signatories of the Convention, including Malta, as well as by EU institutions. In Malta, it is the Data Protection Unit within the Ministry of Justice to be responsible for co-ordinating, advising and assisting as necessary in the implementation of data protection requirements within the Public Service and the Public Sector, as much as ensuring compliance with data protection law.

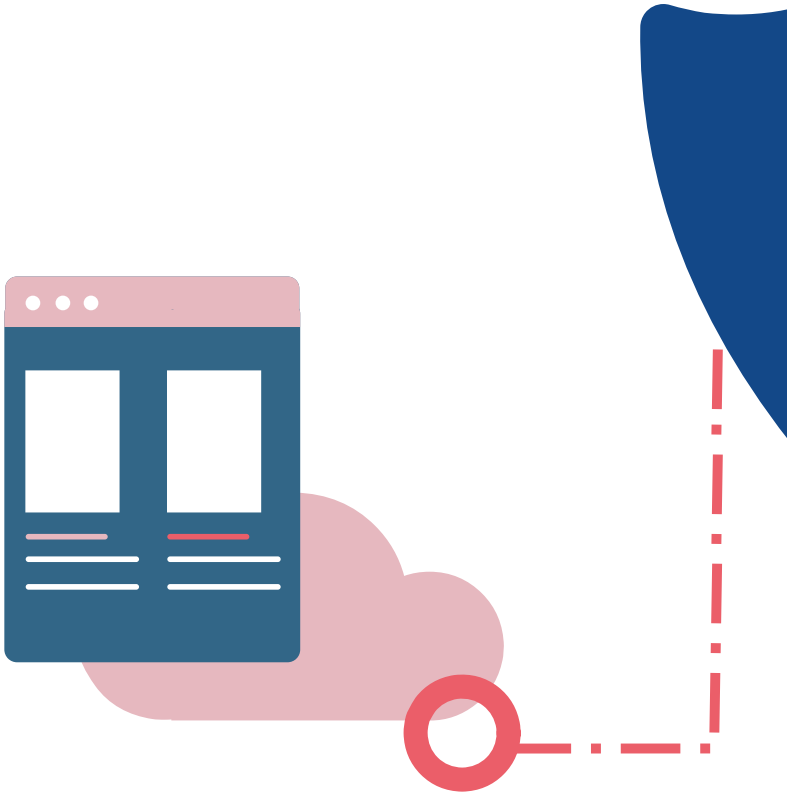
3.3
EU-funded GDPR awareness campaign

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.

In 2020, the IDPC issued a public tender for the delivery of a multilevel awareness-raising campaign, which the IDPC later on implement by:

- airing video-clips on national TV stations in the form of adverts;
- broadcasting messages on national radio stations promoting the importance of data protection in the online environment;
- publishing animations as adverts on online news portals regarding consent prior to posting personal data online;
- using public transport advertising to promote the importance of data protection and the role of the IDPC; and
- publishing sponsored ads on social media to promote the rights of individuals under data protection law.

The IDPC considers the initiative highly beneficial and impactful for controllers, processors and data subjects. As a result, during and after the campaign, the IDPC experienced a spike in the number of queries and complaints.



3.4

New website for the IDPC

After months of strenuous work of content adaptation and creation activities, in 2020 the IDPC finally came up with brand new, modern and user-friendly website. Remarkably, the new website introduced dedicated and guided online forms to file data protection complaints and to notify personal data breaches. As a result, the work of the IDPC was greatly simplified and standardised. At the same time, the public has now at its disposal well-compiled information and guidance and easy-to-use essential tools to seek the assistance of the IDPC where needed.

Guidance and information on the website are divided into two main sections, respectively dedicated to organisations and individuals. Furthermore, in the section "Publications", the IDPC issues updates and news on data protection and its work. In 2020, the IDPC published on this section comprehensive guidance on a number of topics, such as the Schrems II judgement, data protection measures for working remotely during to the COVID-19 pandemic, disclosure of health data in the occupational medicine and data monetisation.

4

Advisory Activities

Nowadays, a vast array regulated sectors have a direct or collateral impact on data protection. Bearing this in mind, the European legislator included amongst the tasks of supervisory authorities that of advising, in accordance with Member State law, the national parliament, the government, and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing.

Consulting the IDPC on data protection aspects during the legislative process is considered to be good practice to ensure that the data protection principles of the GDPR are upheld, and that the necessary safeguards are in place to ensure that the rights and freedoms of the concerned data subjects are not adversely impacted.

The year 2020 has been particularly productive for the IDPC in terms of advice given on proposed legislative measures, which covered several areas such as public health, immigration and citizenship, processing of personal data concerning health, law enforcement, data sharing and re-use and public administration.

4.1
Advice on queries

Compliance with data protection law is a strenuous exercise for controllers and processors, which should commence with a sound understanding of the relevant provisions of law. At the same time, it is important that data subjects are aware of their rights, know what to expect when they entrust controllers or processors with their personal data and make responsible choices in that respect. The IDPC also believes that the work of data protection supervisory authorities should be open, transparent and inclusive.

For these reasons, the IDPC operates both an open telephone line available during business hours and a generic mailbox accepting queries on matters related to data protection and freedom of information.

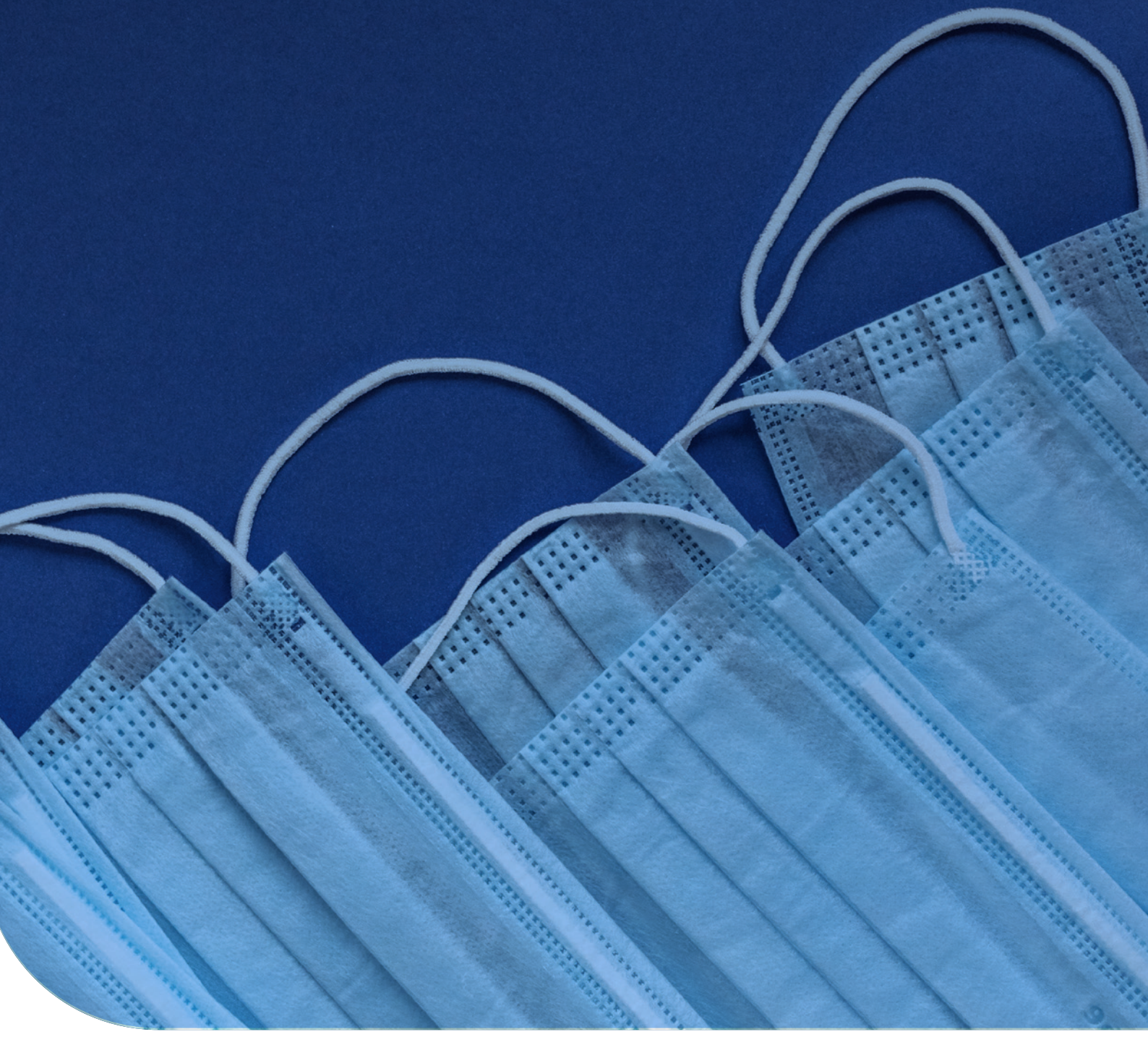
These services are available to private individuals, professionals, organisations, and public entities. In the year 2020, the matters on which the IDPC was consulted the most were:

- processing of personal data by means of video-surveillance devices (CCTV cameras);
- data protection rights, in particular right of access and right to erasure;
- lawfulness of processing;
- personal data transfers from and to the UK after the Brexit; and
- unauthorised disclosure of personal data.

The IDPC strongly encourages the public to make use of these services and it is very much eager to hear suggestions about how these may be improved.

5

COVID-19 Outbreak



5.1

Consultation by Health Authorities on the Covid Alert Malta App

During 2020, Malta opted for the deployment of a Contact Tracing and Alerting Mobile Application, also known as "Covid Alert Malta App". The aim of this project was to strengthen Malta's response to the pandemic by assisting the Health Authorities in automating part of the contact tracing work, alongside traditional contact tracing techniques.

The Health Authorities carried out a data protection impact assessment on the Covid Alert Malta App and submitted a copy of this exercise to the IDPC. The IDPC observed that the Health Authorities had embedded technical solutions in the app to achieve data pseudonymisation, and that they had designed taking into account the risk of re-identification of its individual users. The IDPC established that no formal prior consultation was required on the Covid Alert Malta App, and it issued its favourable opinion about its implementation.

5.2

Updates on IDPC website

In April 2020, the IDPC updated its website by publishing guidance on the application of data protection rules in view of the directives and the advice of the Health Authorities in order to contain and mitigate the effects of the pandemic. The IDPC invited stakeholders to ensure that the rights and freedom of the data subjects are upheld at all times whilst abiding by such measures.

Inevitably, in tackling the pandemic, a substantial quantity of data concerning health is being processed. Data concerning health is classified as a special category of personal data under the GDPR and due to its sensitive nature, it is subject to enhanced safeguards. Article 9 of the GDPR generally prohibits the processing of special categories of personal data, unless an exemption applies. In its publications, the IDPC draw the public's attention on one of these exemptions, which is relevant in relation to the emergency situation arising from the pandemic. Said exemption derives from article 9(2)(i) of the GDPR, by virtue of which the general prohibition to process special categories of personal data shall not apply in the event that processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.

6

Supervisory and enforcement activities

6.1
Data protection complaints

The IDPC is responsible for monitoring the application of the GDPR in Malta and for the enforcement of the rules contained therein. The GDPR gives data subjects the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes the GDPR. One of these supervisory authorities is the IDPC, which receives and resolves hundreds of data protection complaints each year.

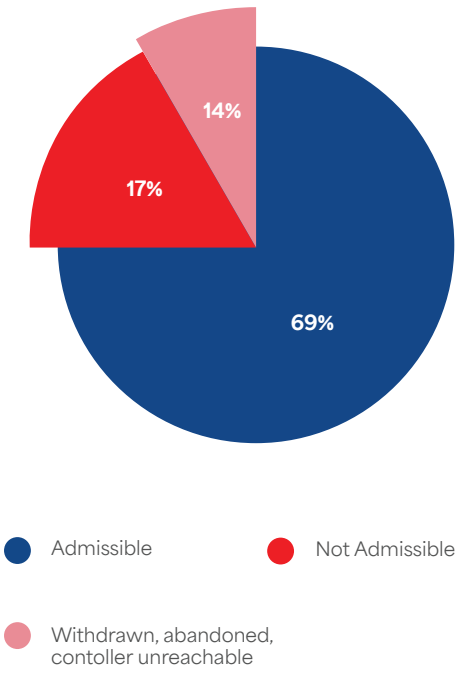
Complaints may be lodged directly by data subjects or by a not-for-profit body, organisation or association acting on behalf of data subjects. Oftentimes, complaints are filed by legal professionals acting on behalf of data subjects. Upon receipt of a complaint, the IDPC carries out a preliminary assessment to determine its admissibility. If the complaint is deemed admissible, the IDPC opens an investigation on the complaint in the context of which it uses its investigative powers under the GDPR as deemed required and it investigates the case to the extent appropriate. In most instances, the IDPC's investigation is concluded with a legally-binding decision issued by the Commissioner and addressed to the parties of the complaint-handling process.

For the purposes of this annual report, complaints are hereby being catalogued as local and cross-border cases.

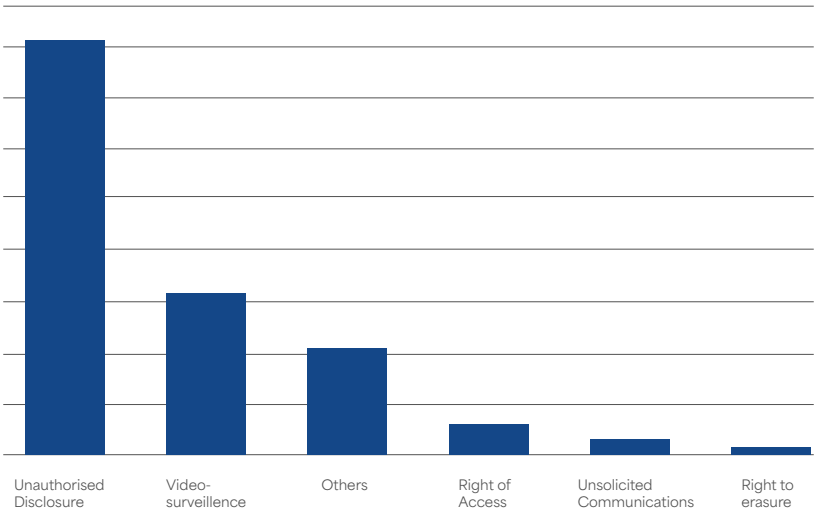
6.1.1 Local cases

Local cases are complaints which do not concern cross-border processing.

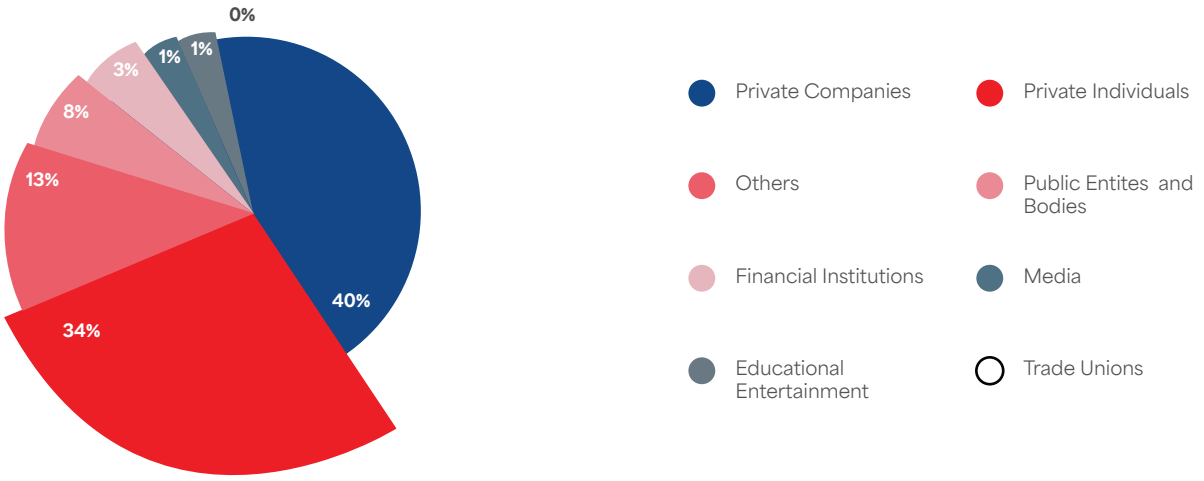
In 2020, the IDPC received a total of 447 local cases, 76 of which were found to be inadmissible and 62 of which were abandoned, withdrawn or not investigated for inability to reach the controller.



As shown in the chart below, complaints concerning unauthorised disclosure of personal data were the most numerous during 2020, followed by other processing of personal data by means of video-surveillance devices (CCTV), exercise of data protection rights and unsolicited communications.

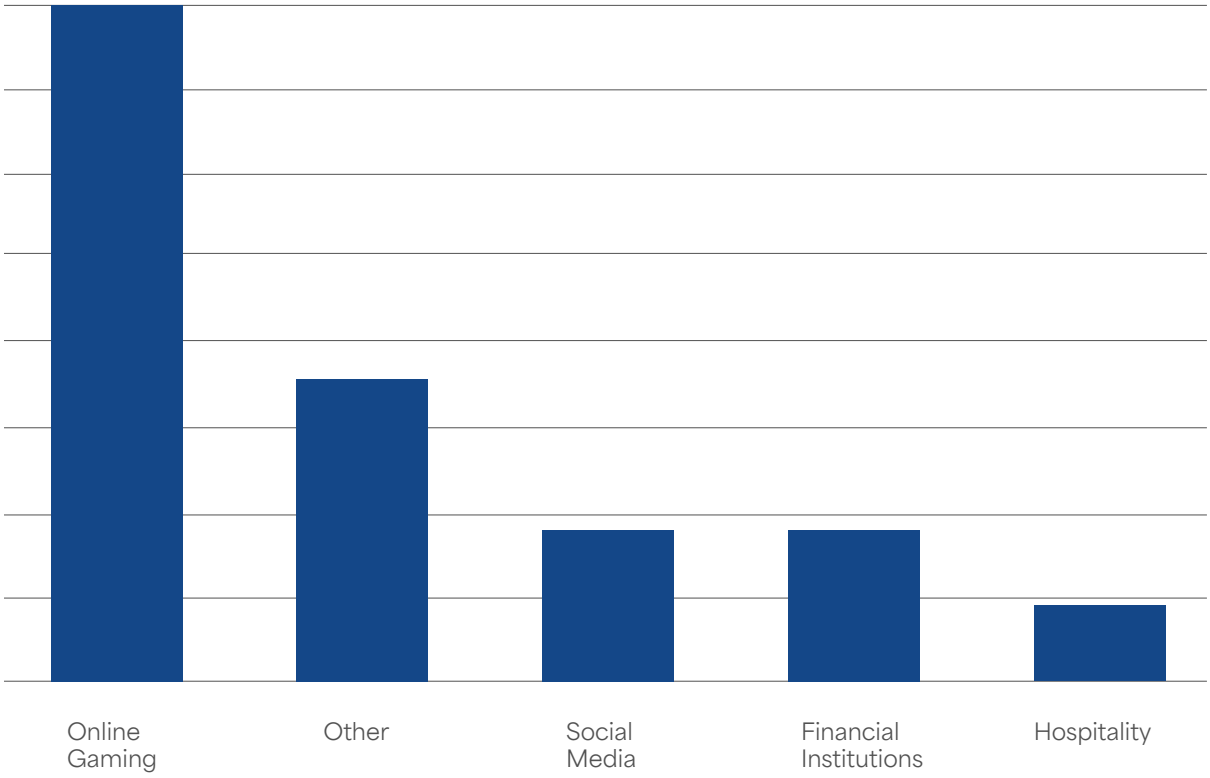


The graph below breaks-down the total number of complaints based on the sector in which the controller-respondent operates. Most of controllers for 2020 were private individuals and private companies.

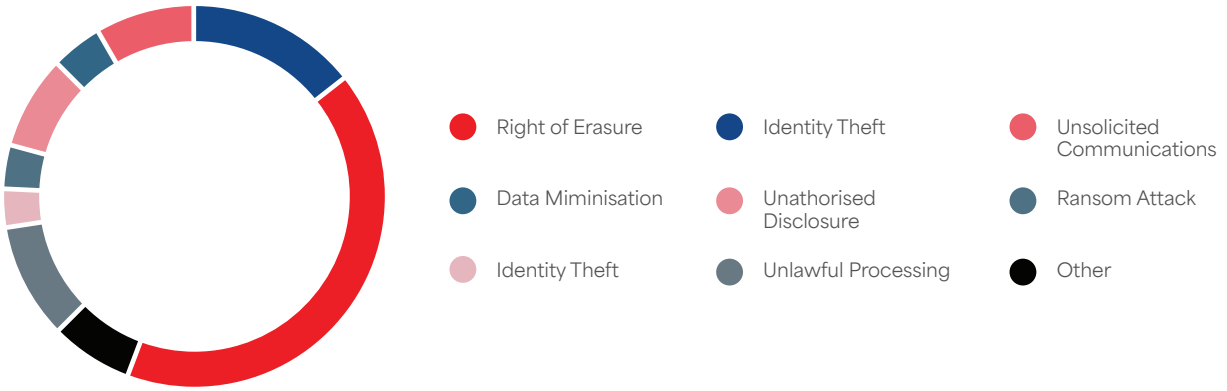


6.1.2 Cross-border cases

With the introduction of the GDPR, the concept of the one-stop shop was established as one of the main innovations. In cross-border processing cases, the supervisory authority in the Member State of the controller's or processor's main establishment, referred to as the "lead supervisory authority" or "LSA", is the authority leading the enforcement of the GDPR for the respective cross-border processing activities, in cooperation with all the authorities which may face the effects of the processing activities at stake, which are called "supervisory authorities concerned" or "CSAs". On the other hand, the complaint-receiving supervisory authority remains the contact point for the complainant in the further course of the complaint-handling process. In order to meet all these requirements, Article 60 GDPR regulates the cooperation procedure between the lead supervisory authority and the other supervisory authorities concerned. The GDPR therefore provides a system of cooperation between the competent authorities, within which they cooperate in order to reach consensus. Overall, this one-stop-shop mechanism is designed to reduce the administrative burden for organisations and make it simpler for individuals to exercise their rights from their home base. In 2020, the IDPC acted as the lead supervisory authority in 16 cross-border cases, with a slight increase from 12 cases in 2019. As can be seen in the figure hereunder, most of the cases relate to organisations operating in the online gaming industry and having their main establishment in Malta.



It is also interesting to observe that, as detailed in the graphic below, the topics of these cases largely concern the exercise of data protection rights, but also security matters such as identity theft and ransom attacks.

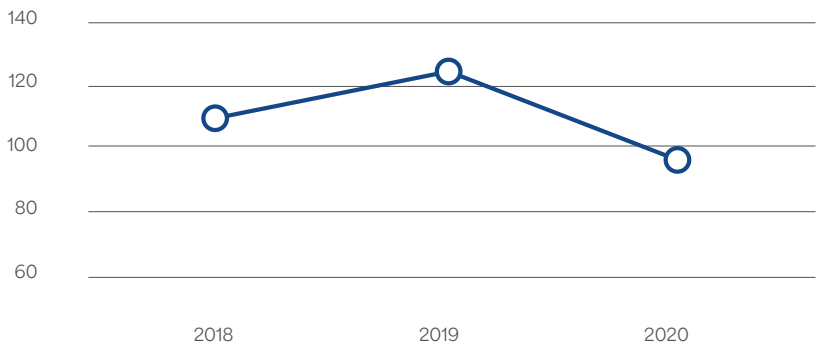


6.2

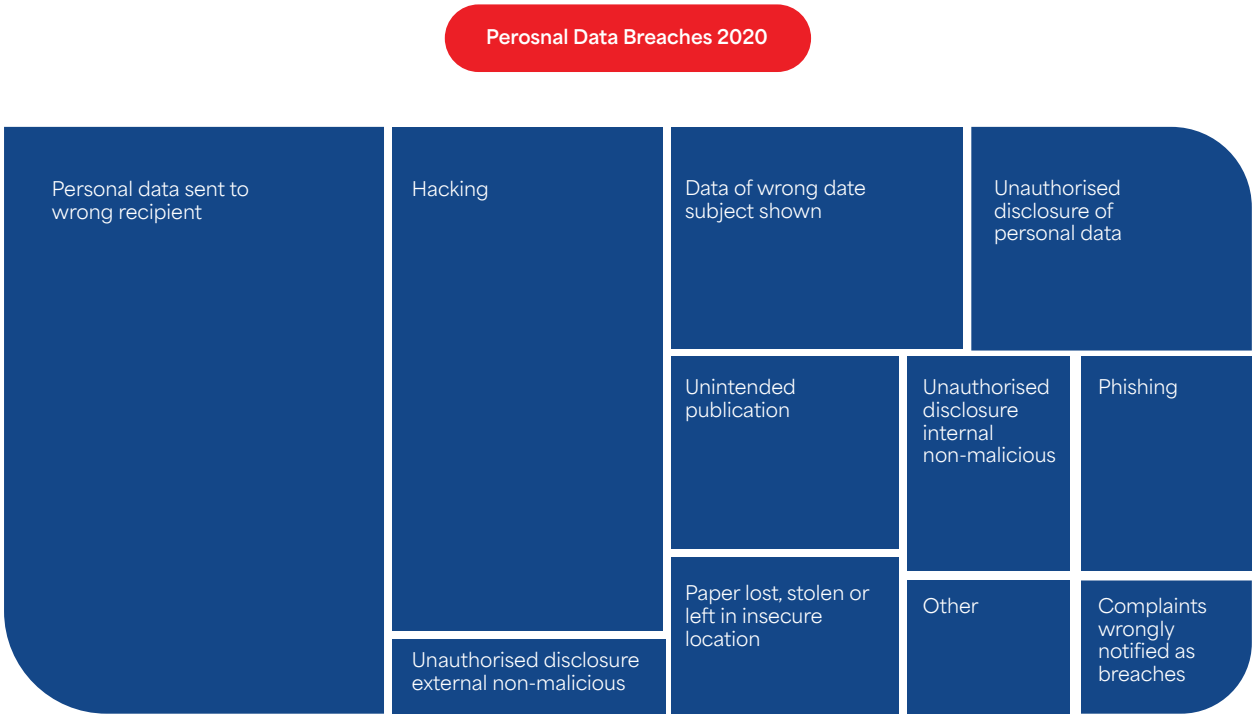
Personal data breaches

The GDPR introduces, in certain cases, the requirement for a personal data breach to be notified to the competent national supervisory authority, and to communicate the breach to the individuals whose personal data have been affected by the breach. The GDPR defines a personal data breach as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed". A breach can potentially have a range of significant adverse effects on individuals, which can result in physical, material, or non-material damage. The GDPR explains that this can include loss of control over their personal data, limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, and loss of confidentiality of personal data protected by professional secrecy. It can also include any other significant economic or social disadvantage to individuals. One of the most important obligations of the controller is to evaluate these risks to the rights and freedoms of data subjects and to implement appropriate technical and organizational measures to address them. The definition of personal data breach and the notification obligation are closely related to the rules in terms of data security which are dictated by the GDPR and to which controllers and processors are subject. The figure below is an overview of the provisions of the GDPR related to data security.

Compared to the previous year, in 2020 the IDPC experienced a little decrease in personal data breach notifications. The below visualises the variation of the number of notifications from 2018, which is the year when the obligation was introduced, to the end of 2020.



It is also interesting to go through the categories of personal data breaches notified to the IDPC in 2020. As visualised below, most of cases relate to personal data sent to the wrong recipient. There is also a notable number of hacking cases, which is a demonstration that the threat and vulnerability landscape is constantly evolving.



If one looks at the sectors to which controllers which notify most of the personal data breaches pertain to, online gaming makes the top of the list. However, as one can notice from the below, personal data breaches affect a large spectrum of industries, both digitally oriented and more traditional.

In 2020, the IDPC received a personal data breach notification concerning a major hacking attack by a company operating in the Information and communication industry. This notification was followed by a substantial number of complaints related to the same matter. Both the data breach and the complaints are under investigation at the time of compiling this report.

6.3

Administrative fines

The GDPR imposes a new, substantially increased level of fines, as well as it provides for harmonization of fines between Member States. On the other hand, under the GDPR, controllers and processors have increased responsibilities to ensure that the personal data of individuals are effectively protected. The GDPR requires that the supervisory authority shall ensure that the imposition of administrative fines shall in each individual case be effective, proportionate and dissuasive. Besides, the GDPR provides a list of criteria to which the supervisory authority shall give due regard when deciding whether to impose an administrative fine and deciding on the amount of the fine in each individual case.

In 2020, the IDPC imposed an administrative fine of €20,000 on a controller for having article 13 and 15 of the GDPR. This was the highest fine which the IDPC issued during the year. The IDPC also fined a controller €15,000 for infringing articles 6, 7, and 21 of the GDPR and Regulation 9 of S.L. 586.01. Other two cases landed with a €5,000 administrative fine each. The first one concerned a request to exercise the right to access upon which the controller failed to provide information on the action taken within one month of receipt of the request, as well as the failure to provide the complainant with a copy of the information pertaining to the complainant. The other case involved unauthorised disclosure of personal data.

6.4

Appeals

Article 26 of the Data Protection Act establishes that any person to whom a legally binding decision of the Information and Data Protection Commissioner is addressed shall have the right to appeal to the Information and Data Protection Appeals Tribunal.

An appeal to the Tribunal may be made on any of the following grounds:

- that a material error as to the facts has been made;
- that there was a material procedural error;
- that an error of law has been made;
- that there was some material illegality, including unreasonableness or lack of proportionality.

Article 29 of the Data Protection Act rules that decisions of the Tribunal may be appealed before of the Court of Appeal by any party and, or by the Commissioner in case they feel aggrieved by any such decision.

In 2020, 9 decisions issued by the Information and Data Protection Commissioner were appealed before the Tribunal.

7

European Affairs

7.1

European Data Protection Board

The role of the EDPB

The European Data Protection Board (EDPB) is an independent European body which contributes to the consistent application of data protection rules throughout the European Union and promotes cooperation between EU data protection authorities. The EDPB is established by the GDPR and is based in Brussels. The Secretariat of the EDPB is provided by the European Data Protection Supervisor (EDPS). The EDPB is composed of representatives of the national supervisory authorities and the EDPS. The supervisory authorities of Iceland, Liechtenstein and Norway are also members of the EDPB on GDPR-related matters. The European Commission and the EFTA Surveillance Authority have the right to participate in the activities and meetings of the EDPB without voting rights.

The EDPB's main tasks and duties are:

- providing general guidance (including guidelines, recommendations and best practices) to clarify the law and to promote a common understanding of EU data protection laws;
- adopting opinions addressed to the European Commission or to national supervisory authorities:
- to advise the European Commission on any issue related to the protection of personal data and new proposed legislation in the European Union. In some instances, the EDPB issue Joint Opinions together with the EDPS;
- to ensure consistency of the activities of national supervisory authorities on cross border matters. If authorities fail to respect an opinion issued by the EDPB, the EDPB may adopt a binding decision;
- adopting binding decisions addressed to national supervisory authorities and aiming to settle disputes arising between them when they cooperate to enforce the GDPR, with the purpose of ensuring the correct and consistent application of the GDPR in individual cases;
- promote and support the cooperation among national supervisory authorities.

EDPB Plenaries and expert sub-groups

During Plenary meetings, which normally take place once a month, EDPB members discuss data protection matters of common interest and relevance and take key decisions on such matters. These can take the form of guidelines, opinions, letters, and so on. In certain instances, to lighten the agenda of Plenary meetings and process non-controversial decisions that could enjoy general consensus more rapidly and efficiently, the EDPB also resorts to the use of written procedures broadcasted through the IMI (Internal Market Information) system. Along with Plenary meetings, which are regularly attended by the Commissioner, the EDPB is aided by the work of expert subgroups (ESGs), which are formed to assist with the performance of the tasks of the EDPB and are given a mandate covering a specific area of data protection. ESGs conduct their work based on a priorly agreed work program intended to cover the most relevant matters falling under their mandate. IDPC's staff routinely takes part to ESGs meetings. For most of 2020, due to the pandemic, both plenary and ESG meetings were held remotely.

In 2020, the following ESGs actively met and carried out their tasks:

Borders, Travel & Law Enforcement (BTLE)	Key Provisions
Compliance, e-Government and Health (CEH)	International Transfers
Cooperation	IT Users
Coordinators	Social Media
Enforcement	Strategic Advisory
Financial Matters	Technology

EDPB taskforces

The EDPB also has the prerogative to create taskforces to work on a single defined task or activity. In 2020, the IDPC participated to the Fining Taskforce, an ad-hoc forum focused on the harmonisation of the calculation of administrative fines. The Fining Taskforce was instituted in 2018 with the purpose of finding a consistent mechanism to calculate administrative fines under the GDPR. To achieve this, in 2020, the Taskforce started to draft a set of guidelines on the calculation of administrative fines under the GDPR. At the time of writing, these guidelines are being worked on.

Following the landmark Schrems II ruling of the of July, on which more details are provided in section 8.3 below, the EDPB also created the Supplementary Measures Taskforce. The work of this expert forum culminated in the EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. The purpose of this document is to assist controllers and processors with, inter alia, on the case-by-case evaluation of the circumstances of the transfer, their duty to identify and implement appropriate supplementary measures to ensure adequate protection when transferring data to third countries, procedural requirements for the implementation of the supplementary measures in addition to an existing transfer tool. At the end of 2020, these recommendations were published on the EDPB website and opened for public consultation. A final version of them is expected to be released next year.

Coordinated Supervision Committee (CSC)

Established within the framework of the EDPB and composed of representatives of the national data protection authorities of each EU Member State and the EDPS, as well as of national data protection authorities of non-EU Members of the Schengen Area when foreseen under EU law, the CSC is tasked with ensuring coordinated supervision of large-scale IT systems and of EU bodies, offices, and agencies. Other functions include exchanging relevant information, assisting supervisory authorities in carrying out audits and inspections and identifying any of their difficulties, as well as examining difficulties of interpretation or application of the EU legal act, drawing up harmonised proposals for solutions to problems, promoting awareness of data protection rights.

7.2

Other EU-level supervisory groups

Customs Information System (CIS) Supervision Coordination Group

The CIS is a computer system centralizing customs information aiming at preventing, investigating and prosecuting breaches of EU customs or agricultural legislation. The CIS is composed of a central database accessible through terminals in each Member State. The data entered in the CIS relate to goods, means of transport, businesses and people associated to such breaches. They also relate to trends in fraud, available competencies, goods detained, seized or confiscated and cash detained, seized or confiscated. The Customs Information System Supervision Coordination Group (CIS SCG) is set up by Regulation (EC) No 766/2008 to ensure a coordinated supervision in the area of personal data protection of the CIS information system. The CIS SCG consists of representatives of the national supervisory authorities of the Member States responsible for data protection, including the IDPC, and the EDPS.

Eurodac Supervision Coordination Group

The Eurodac is an EU fingerprint database established in 2013 for the purposes of identifying asylum seekers and irregular border-crossers. It facilitates the judicious and transparent receipt and processing of asylum applications from those who may need the protection afforded by Europe. It also helps Member States to determine responsibility for examining an asylum application by comparing fingerprint datasets. In order to ensure supervision coordination for Eurodac, representatives of the

national data protection authorities, including the IDPC, and the EDPS meet usually twice a year.

Europol Cooperation Board

In line with Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 (the Europol Regulation), the EDPS has the task to supervise the lawfulness of personal data processing by Europol since 1 May 2017. Following the entry into force of the new Europol Regulation, the EDPS has taken over the supervision of Europol's processing activities, whereas the Europol Cooperation Board (ECB) has been set up in order to facilitate the cooperation between the national supervisory authorities and the EDPS on issues requiring national involvement, thus keeping the legacy created by the former supervision structure operating under the Joint Supervisory Body (JSB) of Europol.

Schengen Information System II (SIS II) Supervision Coordination Group

The SIS II is a large-scale IT-system that is set up under Regulation (EC) No 1987/2006 as a compensatory measure for the abolition of internal border controls, the objective of which is to guarantee a high level of safety within an area of freedom, safety and justice of the European Union, through the enforcement of a public order, and safety and safeguarding of the safety on the territory of the member countries, among other things. SIS II is an information system that enables national law enforcement, judicial and administrative authorities to carry out specific tasks by sharing relevant data. The SIS II Supervision Coordination Group (SCG) is a group set up by the SIS II Regulation with the aim of coordinating supervision in the area of personal data protection. The group is made of representatives from the national supervisory authorities that are responsible for data protection, and of the EDPS. The group meets twice a year usually to share experience, discuss issues of interpretation and/or application of SIS II legal framework and of supervision and, or exercise of rights of data subject, provide assistance in carrying out audits and inspections, and lastly draw up proposals for joint solutions and promote awareness of data protection rights.

Visa Information System (VIS) Supervision Coordination Group

The Visa Information System (VIS) is established under Regulation (EC) 767/2008 for the purpose of facilitating the visa application procedure, prevent visa shopping and fraud, and facilitate border checks as well as identity checks within the territory of the Member States and to contribute to the prevention of threats to the internal security of the Member States. Article 43 of the VIS Regulation lays down the legal basis for cooperation between national supervisory authorities and the EDPS, which cooperation has been formalised under the VIS Supervision Coordination Group, which meets twice a year to allow for cooperation, discuss the new developments in relation to the VIS, and ensure that it maintains adequate levels of effective supervision.

7.3

Brexit and data protection

The withdrawal of the United Kingdom of Great Britain and Northern Ireland from the EU had implications on data protection, taking into account the number of organisations carrying out cross-border processing of personal data from the EU to the UK and vice versa as part as their business operations. As a consequence of the Brexit, the UK has become a third country to the EU for all purposes and intents, including data protection. As a general rule, the GDPR and the Law Enforcement Directive prohibit to transfer personal data from the EU to a third country, unless adequacy decisions in respect of that third country are in place, or appropriate transfer tools are used. On the 24th January 2020, the EU and the UK signed a "Withdrawal Agreement" which introduced a transitional period during which EU law continued to apply in the UK until the 31st December 2020. During this period, personal data flows between the EU and the UK have remained lawful without the need for companies and / or public authorities to put in place any transfer tool under the GDPR or the Law Enforcement Directive to legitimate such transfers. In view of the imminent end of the transition period, on the

24th December 2020 the EU and the UK signed a "EU-UK Trade and Cooperation Agreement" which will be provisionally applicable as of the 1st January 2021. Under the provisions of such agreement, stakeholders that are subject to the GDPR and to the Law Enforcement Directive will be entitled to transfer personal data from the EU (and EEA) to the UK, until adequacy decisions have been adopted, for no more than six months. Reciprocally, and on a transitional basis, the UK has deemed the EU (and EEA) member countries to be adequate to allow for outward data flows from the UK. In the meantime, the UK's Information Commissioner Office, with which the IDPC had established and maintains a solid bilateral relationship, ceased to be a member of the EDPB and to participate in the one-stop-shop cooperation mechanism of the GDPR. It is expected that during the first months of 2021, the European Commission will launch the procedure to adopt adequacy decisions for transfers of personal data to the UK. As part of the procedure, the Commission shall seek the opinion of the EDPB and approval from a committee composed of representatives of the EU Member States before such decisions are formally adopted.

7.4

Conference of European Data Protection Authorities (Spring Conference)

Started back in in the 90's, the Conference of European Data Protection Authorities, also known as the "Spring Conference", was formed with the aim of bringing together the data protection authorities of Europe and other intergovernmental organisations to address practical issues of common interest in relation with the rights to privacy and data protection. With the years passing, and with the evolution of the data protection legislative framework in Europe, the mandate of the Spring Conference has been progressively extended to include matters of more operational nature, such as cooperation between authorities in cross-border cases. In May 2020, the IDPC attended the 29th Edition of the European Conference of Data Protection Authorities which was held in Tbilisi and hosted by the Personal Data Protection Service of Georgia. The conference stimulated a vivid discussion on a number of interesting topics, such as the protection of personal data of children and the processing of personal data by international organisations. The data protection authority of Croatia was given the mandate to host and organise the 30th edition of the Spring Conference, to be held in May 2020. Regrettably, due to the outbreak of the coronavirus, the Croatian authority announced that the conference would be postponed to 2021.

The IDPC is honoured to be a permanent member to the Spring Conference, considering it a precious and high-profile forum to exchange information, expertise and good practices and to debate key data protection matters. The IDPC regrets that the events could not take place as planned and looks forward to meeting the delegations in the upcoming session.

7.5

Council of Europe Consultative Committee (T-PD)

The Republic of Malta is a party to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention ETS no. 108) and a member of the consultative committee (T-PD) set up in terms of Chapter V of the Convention. The T-PD meets biannually, and it is responsible inter alia for making proposals to facilitate or improve the application of the Convention, and to suggest amendments to the same Convention. During the year under review, the IDPC gave its contribution to this international forum by participating to its plenary meetings, which focused on the evaluation and follow-up mechanism under Convention 108+, trans-border access to data in relation to the Budapest Convention on Cybercrime, facial recognition, profiling and data protection in the education systems amongst others.

8

International Affairs

8.1

Global Privacy Assembly

The recently renamed "Global Privacy Assembly" or "GPA" (formerly the "International Conference of Data Protection and Privacy Commissioners") first met in 1979. With the years passing, the GPA has grown exponentially to become a forum which gathers more than 130 data protection and privacy authorities across the globe. The 2020 edition of the Assembly was not immune to the COVID-19 pandemic. Initially planned to be held in Mexico City, the venue was changed to a virtual setting. The event took place in "closed session" format from the 13th to the 15th October 2020. During the first day of the event, the GPA presented the new accredited members and observers and has presented its strategic priorities, identified in:

- advancing global privacy in the digital age;
- maximising the GPA's voice and influence; and
- capacity building.

On the second day, the GPA COVID-19 Taskforce, formed in response of the pandemic, was presented. The taskforce explained its duties and presented a draft Resolution on the Privacy and Data Protection challenges arising from the COVID-19 pandemic. The concluding day of the conference was dedicated to voting procedures and to the adoption of GPA's resolutions. The IDPC joined the GPA as an accredited member in 2003 and since then, it has participated with great interest to the events that the assembly has organised, considering them a unique source to monitor the development and evolution of data protection and privacy law from a truly international perspective.

8.2

Common Thread Network (CTN)

The CTN is a forum aimed at bringing together the data protection and privacy authorities of Commonwealth countries, with representation from Europe, Africa, Asia, the Pacific, the Americas and the Caribbean. In so doing, it facilitates cross-border cooperation and building capacity by sharing knowledge on emerging trends, regulatory changes and best practices for effective data protection.

8.3

Global Privacy Enforcement Network (GPEN)

The IDPC is part of the GPEN since 2015. The GPEN is a network intended to foster cross border cooperation among privacy and data protection authorities. By virtue of a Recommendation adopted in June 2007 by OECD Governments, member countries were mandated to develop an informal network for the specific purpose of exchanging information and discuss practical aspects of enforcement cooperation through a dedicated online platform. In June 2012 the GPEN Action Plan was adopted.

8.4

The British, Irish and Islands' Data Protection Authorities (BIIDPA)

The BIIDPA is an informal meeting held on an annual basis be where the organisation is volunteered by one of the respective participants, being Bermuda, Cayman Islands, the Republic of Cyprus, Gibraltar, Guernsey, the Republic of Ireland, Isle of Man, Jersey, Malta and the United Kingdom. Discussions at these meetings are informal in nature and provide the right platform for the exchange of useful information to ensure a consistent approach to the treatment of issues which are of common interest.

8.5

Berlin Group

The International Working Group on Data Protection in Telecommunications (IWGDPT), also informally referred to as the Berlin Group, was established in 1983 on the initiative of a number of national data protection authorities in the world. The secretariat has since then been provided by the data protection authority of Berlin (Berliner Datenschutz-beauftragter). Membership in the Group is not limited to national data protection authorities but extends also to representatives from the private and NGO sectors. Over the last years, the Group has focused on data protection and privacy related issues of information technology in the wide sense, with a special focus on Internet-related developments.

8.6

International transfers of personal data

The year 2020 was particularly intense in relation to international transfers of personal data. The IDPC did not only attend various meetings at EDPB level on the matter, but also joined countless webinars and online events deadline with the international flow of personal data. The IDPC received a large number of queries on the topic on several related matters, such as for example use cloud infrastructures based in third countries and the provision of access to processors located in a third country. In such cases, the IDPC confirmed the applicability of the conditions laid down in Chapter V GDPR. Considering that awareness of the data flows is the starting point to afford an essentially equivalent level of protection to the data that it transferred, as a rule of thumb, the IDPC has been consistent in advising data exporters to map all their transfers. Transfers must always be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is transferred to and processed in the third country. The next step is choosing the most appropriate transfer tool amongst those listed under Chapter V GDPR. In the event that a country or region is adequate according to a decision issued by the European Commission, it is a good practice to monitor the validity of such adequacy decision over time. In the absence of an adequacy decision, exporters must rely on one of the transfer tools listed under Articles 46 GDPR. As an exception to the general rule, where the transfer is occasional and non-repetitive, controllers may be able to rely on one of the derogations provided for in Article 49 GDPR, provided that all the conditions laid down therein are complied with.

8.7

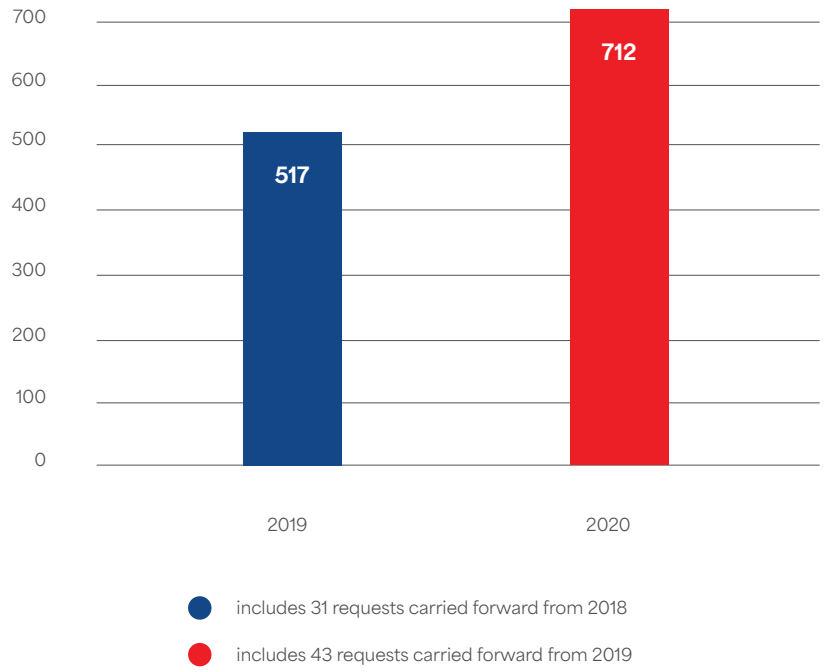
Schrems II ruling

In July 2020, the Grand Chamber of the Court of Justice of the European Union issued a ruling in the case Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, which originated from a request for a preliminary ruling from the High Court of Ireland. The judgement, commonly referred to as “Schrems II”, is particularly relevant in relation to international data transfers. In Schrems II, the Court analysed the EU-US Privacy Shield to determine that US laws did not provide for an essentially equivalent, and therefore sufficient, level of protection as guaranteed by the GDPR and the EU Charter of Fundamental Rights. According to the Court, the legal bases of certain US surveillance programmes were not limited to what is strictly necessary and would be considered a disproportionate interference with the rights to protection of data and privacy, since they did not sufficiently limit the powers conferred upon US authorities and lacked actionable rights for EU subjects against US authorities. The Court also ruled that the Ombudsman mechanism under the EU-US Privacy Shield did not provide data subjects with any cause of action before a body which offers guarantees substantially equivalent to those required by EU law, such as to ensure both the independence of the Ombudsperson provided for by that mechanism and the existence of rules empowering the Ombudsperson to adopt decisions that are binding on the US intelligence services. On these grounds, the Court declared the EU-US Privacy Shield decision invalid. Moreover, the Court stipulated stricter requirements for the transfer of personal data based on standard contractual clauses. Thereafter, controllers and processors that intend to transfer data based on standard contractual clauses must ensure that data subjects whose personal data are being transferred are granted a level of protection essentially equivalent to that guaranteed by the GDPR and by the, if necessary, with additional measures to compensate for lacunae in protection of third-country legal systems. Failing that, operators must suspend the transfer of personal data outside the EU.

9

Freedom of Information

During 2020, the total number of requests received by Public Authorities from applicants exercising their right to access information by virtue of the Freedom of Information Act had a significant increase in comparison with the previous year, as shown in the chart below.



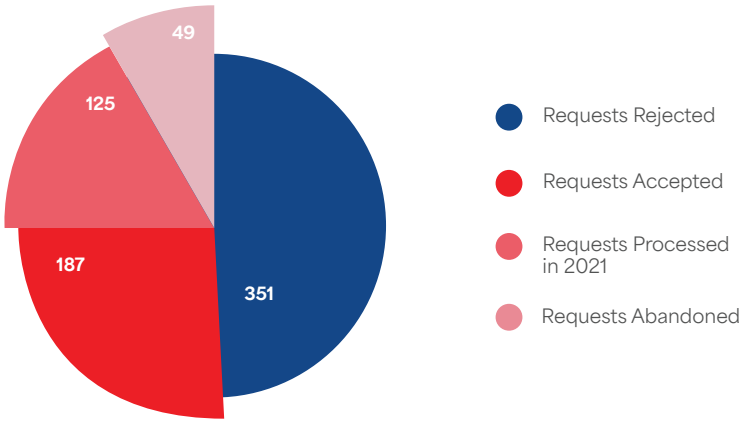
The percentage increase of total FOI requests received by public authorities in 2020 in comparison to 2019 was of 37.7%.

In 2020, it took public authorities in receipt of FOI request an average of 22 days to process such requests.

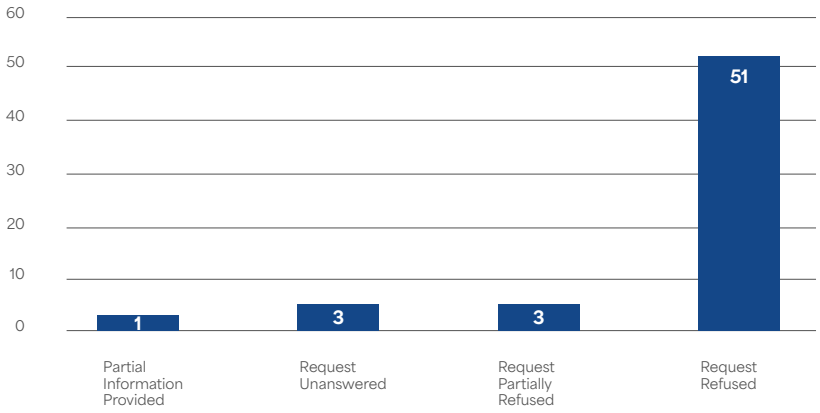
In 2020, public authorities accepted 187 FOI requests and rejected 351 of them. In addition to this, 43 requests were abandoned, and 125 requests were processed in 2021.

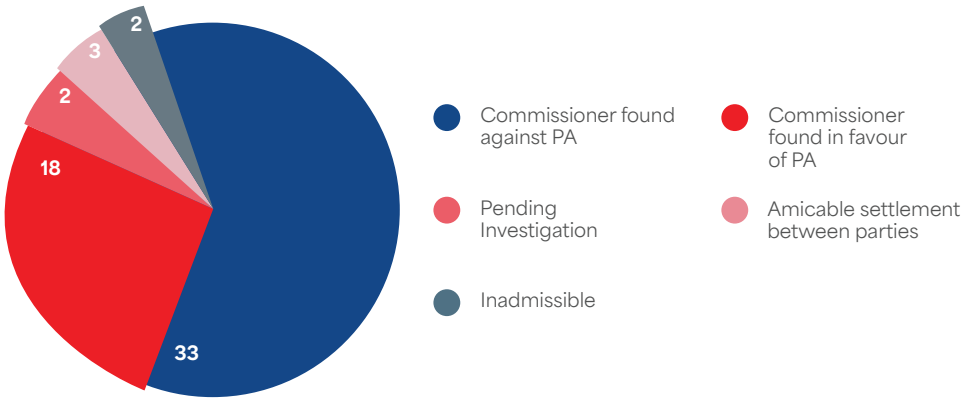
The main reasons invoked by public authorities for rejecting requests and the corresponding numbers are being listed below.

Document requested is excluded from the scope of the FOI Act by virtue of Article 5 **(Art. 14(a) Cap. 496)**	56
Document requested is publicly available or will be published within three months **(Art. 14(d) Cap. 496)**	59
Document requested cannot be found **(Art. 14(e) Cap. 496).**	31
Resources required to identify, locate or collate the document or documents would substantially and unreasonably divert the resources of the authority for its operations **(Art. 14(f)(i) Cap. 496)**	1
Document requested is not held by the public authority, or connected more closely with the functions of, another public authority **(Art. 14(g) Cap. 496)**	114
Request is considered frivolous, trivial or vexatious **(Art. 14(h) Cap. 496)**	2
Other reasons	88
TOTAL	**351**



In 2020, the IDPC received a total of 58 complaints pursuant to the FOI Act. The reasons of applicants for filing such complaints are compiled in the graph hereunder.





In relation to such complaints, during 2020, the Commissioner issued fifty-three (53) Information Notices, forty (40) Decision Notices and three (3) enforcement notices. These were issued both in relation to complaints carried forward from 2019 and to complaints commenced to be investigated in 2020.

In 2020, no appeals before the Information and Data Protection Appeals Tribunals were filed against decisions issued by the IDPC.

Financial Statements

Commissioner's Report

For the Year Ended 31 December 2020

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 2020.

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 £53,326 (2019: a deficit of £6,923) before taking into account the result from the collection of notification fees. The Office received Government subvention amounting to £550,000 in 2020, representing an increase of 14.6% when compared to 2019. Total administrative expenditure amounted to £515,281, resulting in an increase of 6.1% when compared to 2019. 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 will no longer have the obligation to pay notification fees to the Office. In 2020, the Office did not collect any notification fees.

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

Going Concern

The Office has considered the potential impact of the recent COVID19 outbreak on the Office's business. Taking into consideration that the Office's main revenue stream is the government subvention, it was concluded that there will not be a significant impact on its operational performance. Therefore, 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

There were no material events affecting the Office which occurred after the reporting date.

Commissioner

Mr. Ian Deguara was appointed Commissioner on 21 December 2020. The former Commissioner was Mr. Saviour Cachia who served up until 14 October 2020. Between the period starting 15 October 2020 until 20 December 2020, pursuant to Article 14(4) of the Data Protection Act, Mr. Ian Deguara, in his capacity of Deputy Commissioner, performed the duties of Commissioner and exercised his powers in accordance with the provisions of Article 53(2) of the Regulation.

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, 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 09 July 2021 and signed on its behalf by:

Mr. Ian Deguara

Commissioner

Registered Address:

2, Airways House, High Street, Sliema SLM 1549, Malta

Independent Audit Report

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 2020, 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 balance sheet of the Office as at 31 December 2020, 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 Companies Act (Cap. 386).

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 Auditors' 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 IFRS, 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.

Auditors' 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.

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 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 auditors'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

09 July 2021

Statement of Comprehensive Income

For the Year Ended 31 December 2020

	Note	2020 €	2019 €
Government subvention		550,000	480,000
Administrative expenses		(515,281)	(485,488)
Finance costs		(728)	(1,435)
Other income		19,335	-
Surplus/(Deficit) for the year	4.	**53,326**	**(6,923)**
Result from collection of notification fees	3.	-	(30,504)
Total result transferred to retained funds		**53,326**	**(37,427)**

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

Statement of Financial Position

As at 31 December 2020

	Note	2020 €	2019 €
ASSETS			
Noncurrent assets			
Property, plant and equipment	7.	408,789	42,500
Current assets			
Trade and other receivables	8.	3,909	-
Cash and cash equivalents	9.	139,558	234,141
Total current assets		143,467	234,141
TOTAL ASSETS		552,256	276,641
EQUITY AND LIABILITIES			
Equity			
Retained Funds		93,562	40,236
Total equity		93,562	40,236
Liabilities			
Noncurrent liabilities			
Deferred income	11.	-	77,506
Trade and other payables	10.	335,348	-
Total noncurrent liabilities		335,348	77,506
Current liabilities			
Trade and other payables	10.	123,346	74,347
Deferred income	11.	-	84,552
Total current liabilities		123,346	158,899
TOTAL EQUITY AND LIABILITIES		552,256	276,641

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 09 July 2021 and were signed on its behalf by:

Mr. Ian Deguara

Commissioner

Statement of Changes in Equity

For the Year Ended 31 December 2020

	Retained Funds €
Balance as at 01 January 2020	40,236
Comprehensive income	
Profit for the year total comprehensive income	53,326
Balance as at 31 December 2020	93,562

	Retained Funds €
Balance as at 01 January 2019	77,663
Comprehensive income	
Loss for the year total comprehensive income	(37,427)
Balance at 31 December 2019	40,236

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

Statement of Cash Flows

For the Year Ended 31 December 2020

	Note	2020 €	2019 €
Cash from operating activities:			
Surplus/Deficit from operations		53,326	(37,427)
Interest expense		728	1,435
Depreciation		31,867	26,195
Decapitalisation of assets		-	729
Profit/(loss) from operations		85,921	(9,068)
Movement in trade and other receivables		(3,909)	7,922
Movement in trade and other payables		(140,430)	158,126
Net cash flows (used in)/from operating activities		(58,418)	156,980
Cash flows from investing activities:			
Payments to acquire property, plant and equipment		(35,437)	(11,940)
Net cash flows used in investing activities		(35,437)	(11,940)
Cash flows from financing activities:			
Payments of interest classified as financing		(728)	(1,435)
Net cash (used in)/from cash and cash equivalents		(94,583)	143,605
Cash and cash equivalents at beginning of year		234,141	90,536
Cash and cash equivalents at end of year	9.	139,558	234,141

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

Notes to the Financial Statements

For the Year Ended 31 December 2020

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.

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.

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.
- The Office has adopted the following new and amended IFRS and IFRIC interpretations:
- IAS 1 and IAS 8 (Amendments) Definition of material (effective for annual reporting periods beginning on or after 1 January 2020).
- IFRS 9, IAS 39 and IFRS 7 (Amendments) Interest Rate Benchmark Reform Phase 1 (effective for annual reporting periods beginning on or after 1 January 2020).
- IFRS 3 Business Combinations (Amendments) Definition of a Business (effective for annual reporting periods beginning on or after 1 January 2020).

Amendments to references to the Conceptual Framework in IFRS standards.

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 the financial statements.

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 4 (Amendments) Insurance Contracts deferral of IFRS 9 (applicable for annual periods beginning on or after 1 January 2021).
- IFRS 9, IAS 39, IFRS 7, IFRS 4 and IFRS 16 (Reform) Interest rate benchmark reform Phase 2 (applicable for annual periods beginning on or after 1 January 2021).
- IFRS 16 (Amendments) Covid 19 related rent concessions (applicable for annual periods beginning on or after 1 June 2020).

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

- IFRS 17 Insurance Contracts (effective for annual reporting periods beginning on or after 1 January 2023)
- IFRS 3 (Amendments) - Business Combinations: Reference to the Conceptual Framework (effective for annual reporting periods beginning on or after 1 January 2022)
- IAS 1 (Amendments) - Presentation of Financial Statements: Classification of Liabilities as Current or Non current (effective for annual reporting periods beginning on or after 1 January 2023)
- IAS 16 (Amendments) - Property, Plant and Equipment: Proceeds before Intended Use (applicable for annual periods beginning on or after 1 January 2022)
- IAS 37 (Amendmens) - Provisions, Contingent Liabilities and Contingent Assets: Onerous Contracts (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 is still assessing the effect of these changes on the financial statements.

Notes to the Financial Statements (Continued)

For the Year Ended 31 December 2020

2. Significant Accounting Policies

a. Going concern

The Office has considered the potential impact of the recent COVID 19 outbreak on the Office's business. Taking into consideration that the Office's main revenue stream is the government subvention, it was concluded that there will not be a significant impact on the Office's business. Therefore, 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.

b. 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.

c. 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.

d. 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.

e. 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.

f. 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 amountoutstanding.

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.

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.

g. Trade and other receivables

Trade 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 Company will not be able to collect all amounts due to the original terms of the receivables.

h. 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.

i. Provisions and contingent liabilities

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

j. Trade payables

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

k. Revenue recognition

i. Government grants

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.

ii Notification fees

Notification fees relating to the current financial year are recognised as revenue on accruals basis. Fees received in advance are accounted for as deferred income.

iii. Interest income

Interest income from investments is accrued on a time basis, by reference to the principal outstanding and at the interest rate applicable.

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

3. Result from collection of notification fees

	2020	2019
	€	€
Revenue from Notifications	-	443
Income from Fines for Late Payment of Notification Fees	-	42,000
Reimbursement of Notification Fees to Government (note 1)	-	(73,506)
Provision for doubtful debts	-	559
Total	-	(30,504)

Note 1: The Office of the Information and Data Protection Commissioner reached an agreement with the Government of Malta that as from 1 January 2016, any income received from the payment of notification fees will be reimbursed back to the Government in return for an increase in Government subvention. This agreement is still in force as of today.

4. Surplus/(Deficit)

Surplus/(Deficit) is charged after charging the following:

	2020	2019
	€	€
Auditors remuneration	2,065	2,065
Depreciation expense	31,867	26,194
Total	33,932	28,259

5. 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 awarded by the Ministry of Finance.

6. Wages and Salaries

a. Wages and salaries

Payroll costs for the year comprise of the following:

	2020	2019
	€	€
Wages and Salaries	407,635	347,556
Total	407,635	347,556

b. Average number of employees

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

	2020	2019
Commissioner	1	1
Directly Employed by the Office	11	9
Total	12	10

7. Property, plant and equipment

	Right of use assets €	Furniture and fixtures €	Motor vehicles €	Office equipment €	Computer software €	Air conditioners €	Total €
Cost							
Opening balance	169,917	51,615	17,400	59,830	13,117	2,520	314,399
Additions	362,719	15,955	-	7,656	11,826	-	398,156
Balance at 31 December 2020	532,636	67,570	17,400	67,486	24,943	2,520	712,555
Depreciation							
Opening balance	(148,678)	(40,597)	(17,400)	(50,071)	(13,117)	(2,036)	(271,899)
Depreciation	(21,239)	(3,694)	-	(3,815)	(2,957)	(162)	(31,867)
Balance at 31 December 2020	(169,917)	(44,291)	(17,400)	(53,886)	(16,074)	(2,198)	(303,766)
Net Book Value							
At 31 December 2019	21,239	11,018	-	9,759	-	484	42,500
At 31 December 2020	362,719	23,279	-	13,600	8,869	322	408,789

8. Trade and other receivables

	2020 €	2019 €
Notification fee receivables	222,374	222,374
Provision for doubtful debts for notification fees	(222,374)	(222,374)
Accrued Income	2,249	-
Prepayments	1,660	-
Total	3,909	-

9. Cash and cash equivalents

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

	2020 €	2019 €
Cash on hand	214	516
Bank balances	139,344	233,625
Total cash and cash equivalents	139,558	234,141
Total cash and cash equivalents in the statement of cash flows	139,558	234,141

10. Trade and other payables

	2020	2019
	€	€
Trade payables	-	2,884
Amount payable to related parties (Note 12)	65,047	42,000
Accruals	30,928	5,192
Lease liability	27,371	24,271
Total	123,346	74,347

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

11. Deferred income

	2020	2019
	€	€
Deferred income	-	162,058
Split as follows:		
Current	-	84,552
Noncurrent liabilities	-	77,506
	-	162,058

The deferred income represents income received by the Office of the Information and Data Protection Commissionerin relation to EU funds for the EU GDPRights project implementation. These funds were to be received into the line Ministry's account. Therefore, in year 2020, a transfer of funds from the Office of the Information and Data Protection Commissioner to the line Ministry's account was affected, bringing the deferred income balance to nil.

12. 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.

11. Deferred income (Continued)

Schedules

Schedule of Administrative Expenses

	2020	2019
	€	€
Wages and Salaries	407,635	347,556
Accountancy Fees	13,821	10,283
Auditors remuneration	2,065	2,065
Advertising Fees	2,481	2,297
Cleaning of premises	2,395	2,598
Consumables	3,839	3,519
Water and Electricity Fees	2,386	1,589
Car Hire Expenses	7,161	5,844
Insurance	49	133
IT expenses	2,044	-
Fuel Expenses	3,775	4,087
Legal Fees	438	1,151
Printing, Postage and Stationery Fees	4,289	6,740
Repairs and Maintenance Fees	8,821	6,857
Internet Subscription Fees	721	1,876
Telephone Fees	6,159	5,961
Travelling Fees	6,224	42,254
Parking Fees	2,962	5,790
Registration Fees	1,051	3,234
Hospitality Costs	162	-
General and Incidental Expenses	4,393	4,948
Bank charges	543	512
Depreciation and Amortisation	31,867	26,194
Total	515,281	485,488

Schedules do not form part of the audited financial statements.

idpc.

INFORMATION AND DATA
PROTECTION COMMISSIONER