

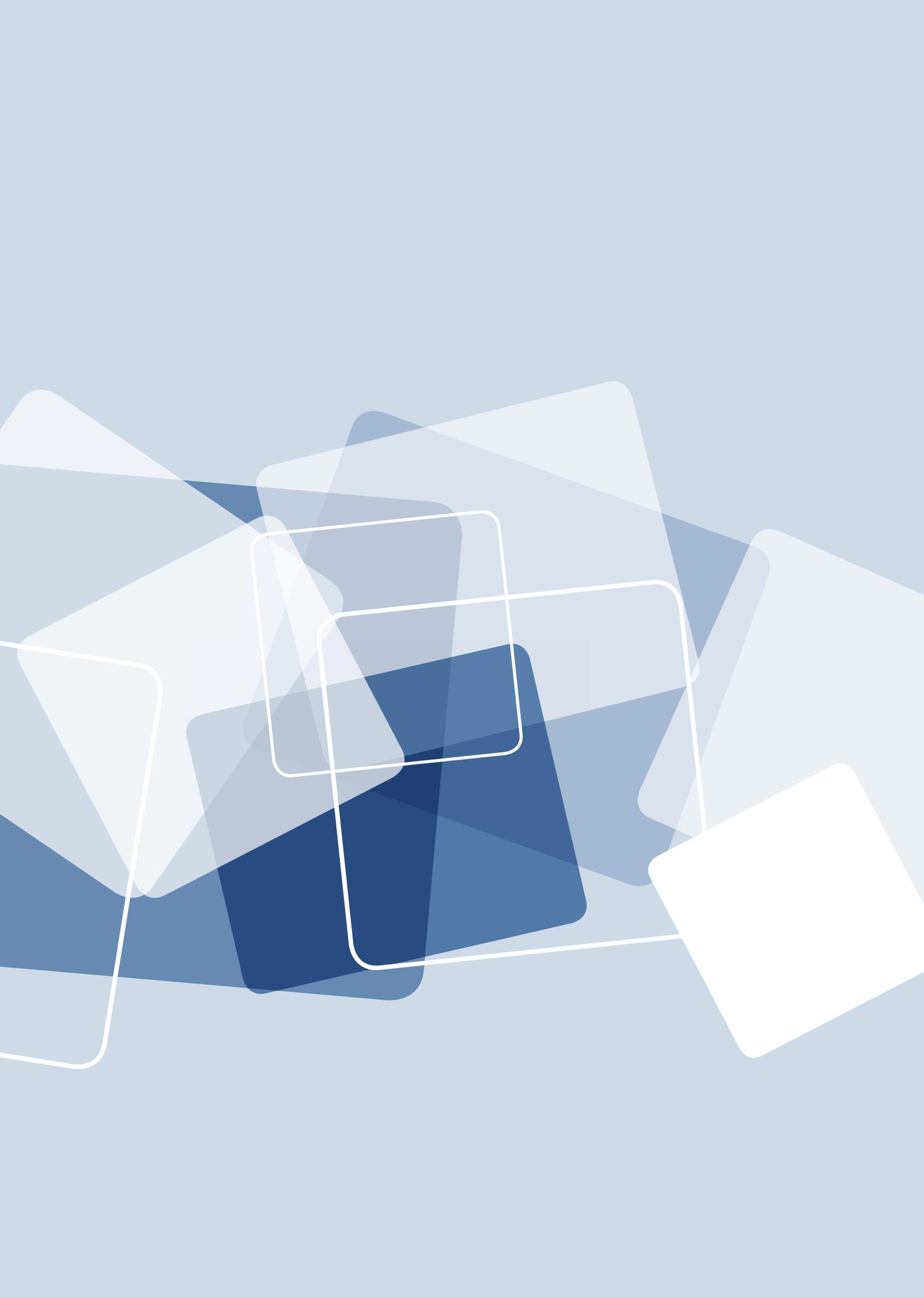


Annual
Report
2018



Contents

1.	Foreword	5
2.	Legislative Background	7
2.1	Data Protection legal framework	9
2.2	Police Directive	9
2.3	Convention 108 and Convention 108+	10
3.	Public awareness	11
3.1	Activities	13
3.1.1	<i>Presentations</i>	13
3.1.2	<i>Discussions with Data Controllers</i>	13
3.1.3	<i>Local TV, Radio and other media</i>	13
3.1.4	<i>IDPC Website</i>	13
3.2	Data Protection Day	13
3.3	Drafting of guidelines together with various sectors	14
4.	Enforcement of the GDPR and handling of case work	15
4.1	Handling of complaints with a national impact	17
4.2	Personal Data Breaches	18
4.3	Enforcement action	18
4.3.1	<i>Administrative fines</i>	19
4.3.2	<i>Other action taken</i>	19
4.4	Cross Border Cases	19
4.4.1	Appeals	20
5.	European and International activities	21
5.1	European Data Protection Board (EDPB)	23
5.2.	EDPB – Expert Sub-groups	23
5.2.1	<i>Borders, Travel and Law Enforcement Subgroup (BTLE)</i>	23
5.2.2	<i>Technology expert sub-group</i>	24
5.2.3	<i>IT Users subgroup</i>	24
5.2.4	<i>Fining Task Force</i>	24
5.3.	International Conference	24
5.4.	European Data Protection Conference	24
5.5	Europol Cooperation Board	24
5.6	Joint Supervisory Body of Eurojust	24
5.7	Schengen Information System II Supervision Coordination Group (SIS II SCG)	25
5.8	Visa Information System Supervision Coordination Group (VIS SCG)	25
5.9	Eurodac Supervision Coordination Group (Eurodac SCG)	25
5.10	Customs Supervision	26
5.11	Council of Europe Consultative committee (T-PD)	26
6.	Freedom of Information	27
	Appendix 1 Organisation Chart	30
	Appendix 2 Financial Statements	31





Foreword

The year 2018 is a milestone in the field of data protection as, on the 25th of May, we mark the date when Regulation (EU) 2016/679, referred to as the General Data Protection Regulation (GDPR) is brought into application across all Member States. The new framework raises the bar across the EU and beyond, in respect of data protection rights for the data subjects, obligations for the data controllers and tasks and powers for supervisory authorities or as they are better known as data protection authorities.

I am proud and satisfied that, on the 28th of May, Parliament has unanimously approved and passed from all its procedural stages, the Data Protection Act, Chapter 586 of the Laws of Malta, the national legislation which implements the relevant provisions of the GDPR. This is a great achievement for my country and puts us on the same level as other EU member states for keeping with the date when the GDPR came into application. This also means that Malta has adapted to the changes brought about by the GDPR.

Large volumes of data are processed anywhere in the world wide web and in every format. Gone are the days where processing of personal data remain local. Today we speak of Big Data, block chain, cloud services and Artificial Intelligence. Indeed, rapid technological developments and globalisation prompted new challenges to the rebalancing of rights in the digital world. The need for more accountability and stronger enforcement for more effective protection to bring about consistency and harmonisation across the EU is more evident than ever.

The processing of personal data is one of the most important factors to achieve the right economies of scale in an ever increasing competitive environment, where globalisation and technology have rendered the world in a single market. Having a strong and more coherent data

protection framework creates public trust and confidence, reduces financial and reputational risks and gives market operators the competitive edge. It is good for business and public services. In this context, the data protection sphere has transformed beyond recognition even though principles remained more or less the same.

Prior to the bringing into application of the GDPR, this Office was heavily engaged in the preparation for the implementation of this legal framework both in the private and public sector. Meetings and seminars were organised where representatives from this Office were the main contributors.

A special word of thanks and praise goes to my staff who, although being the smallest data protection authority in the EU, together as a team, we still managed to maintain a high level of quality and professional service. I therefore wish to acknowledge their dedication in the specialised work they deliver and look forward to the new challenges that next year will bring in the data protection landscape.

Saviour Cachia
Commissioner

Mission Statement

The Commissioner's mission is "to afford individuals with their right to data protection against the violation of their privacy by the processing of personal data, as well as, to facilitate the right to access information held by public authorities to promote added transparency and accountability in government."

His vision is "to have an open society in which individuals feel confident that their right to personal data protection is safeguarded whilst also enjoying their right to freedom of information, to strengthen their rights and freedoms of the individuals and enhance democracy through the establishment of those human rights."

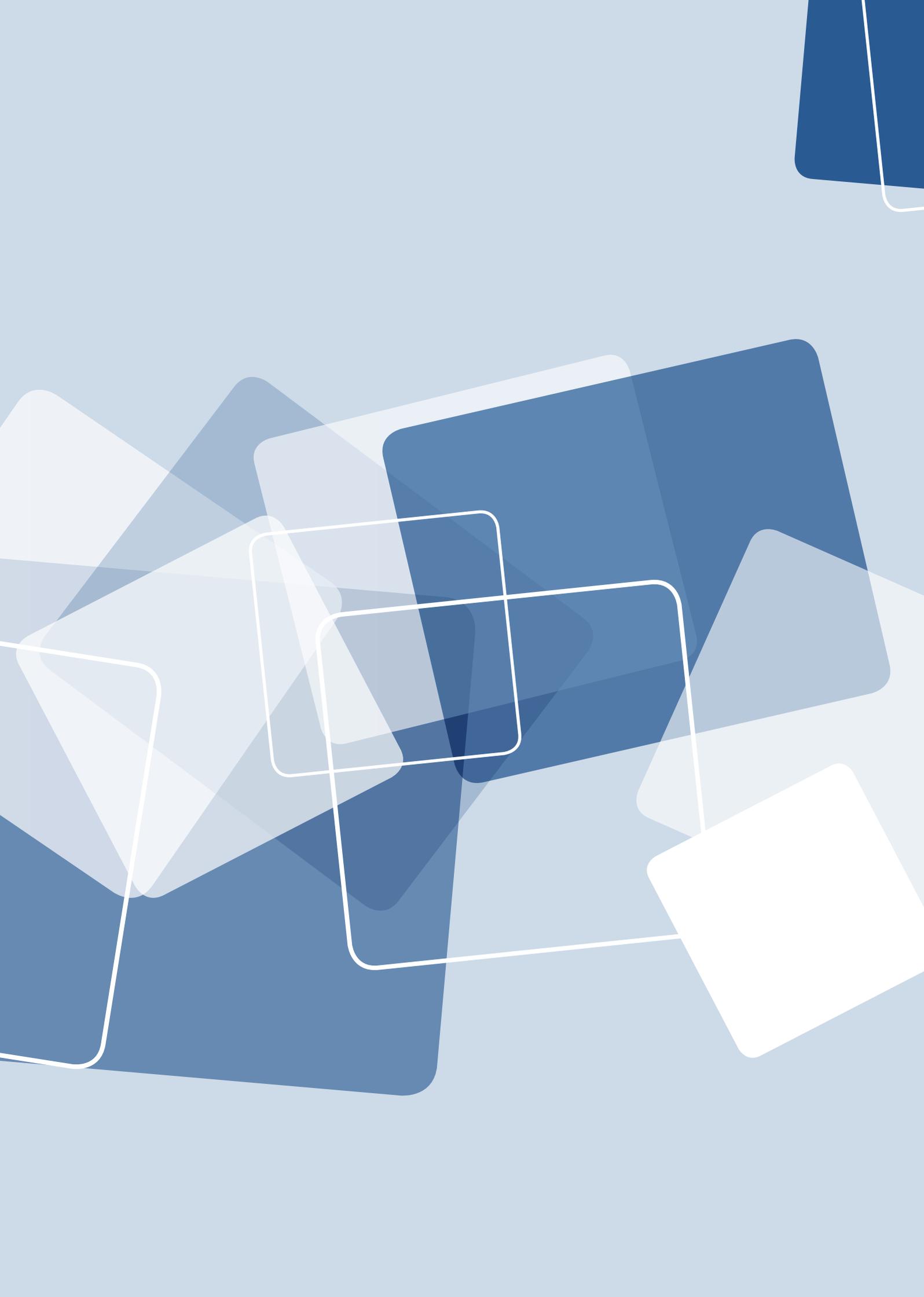
In line with his mission and vision, the Commissioner is resolute to deliver on the following principal objectives which shall form an integral part in the discharge of his core tasks and duties:

- ensures that every data subject's privacy and data protection rights are fully safeguarded and respected;
- regulates data controllers in the public and private sectors in an effective manner;
- investigates, in a fully independent and impartial manner, data protection and freedom of information complaints;
- strives to take initiatives to raise data protection awareness;
- contributes to the consistent application of the GDPR by cooperating with his European Counterparts through the consistency mechanism;
- provides any person with the necessary guidance and assistance in relation to data protection rights and obligations;
- ensures that every public authority upholds acceptable standards to ensure transparency and good governance in the conduct of their operations;



2

Legislative Background



2

Legislative Background

2.1 Data Protection legal framework

Directive 95/46/EC of the European Parliament and Council of the 24th October 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data was transposed into Maltese legislation on the 14th December 2001, under the Data Protection Act, Chapter 440 of the Laws of Malta. The Act was completely brought into effect in July 2003. This Act also conformed to the Convention of the Council of Europe for the protection of individuals regarding automatic processing of personal data (ETS NO 108) ratified in 2003.

The period under review was marked by preparations to monitor and enforce the application of the General Data Protection Regulation which became applicable on the 25th May 2018, two years after its adoption. The GDPR brings about a new generation of data protection rules together with enhanced rights for the data subjects including the right to know what information is held about them and the right to be forgotten. The rules laid down in the GDPR, also brought about a number of significant changes in how organisations approach data protection. One can mention for instance the principle of accountability in that all controllers must ensure that they are able to show compliance with the provisions of the regulation. Indeed, controllers have an increased onus in taking a proactive approach insofar as data protection is concerned. It is also important to mention the greater enforcement powers which are granted to the supervisory authorities which have definitely helped to establish a higher level of compliance.

After a period of intense preparation, Government introduced a draft bill that was brought into force on the 28th May 2018 by virtue of Act XX of 2018 - 'The Data Protection Act' (CAP. 586). This Act, which implements and further specifies the relevant provisions of the General Data Protection Regulation, repeals and replaces the aforementioned Directive 95/46 as transposed by the 'Data Protection Act' CAP.440. Implementing the new legislative framework on data protection offered new and greater challenges to this office and, consequently care was taken to ensure a smooth introduction as possible.

The coming into force of the Act brought with it various legislative developments, insofar as subsidiary legislation is

concerned. The previously mentioned 'Processing of Personal Data (Electronic Communications Sector) Regulations' including all its amendments, 'Processing of Personal Data (Protection of Minors) Regulations' and 'Processing of Personal Data (Education Sector) Regulations', now form part of the new Data Protection Regime and have been renumbered as Subsidiary Legislation 586.01, 586.04 and 586.07 respectively. Two new regulations were also introduced to provide for restrictions on the data protection rights pursuant to Article 23 GDPR and to set out further conditions on the processing of data concerning health for insurance business purposes.

2.2 Police Directive

On 14th April 2016, the European Parliament and the Council reached an agreement on the Directive 2016/680 on 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, including the safeguarding against and the prevention of threats to public security. In accordance with Article 63 of the Directive, Member States were obliged to transpose the Directive by 6 May 2018. This Directive is not a full harmonisation legislation, which means that Member States may introduce higher data protection safeguards.

In order to ensure the timely transposition, the Ministry for Home Affairs and National Security (MHAS) had set up an inter-ministerial committee, which was composed of members from the Malta Police Force, Ministry for Justice, Culture and Local Government (MJCL), the Office of Information and Data Protection Commissioner (IDPC), the Data Protection Unit (MJCL) and the Attorney General's Office. Consultations were also undertaken with the Customs Department, the Financial Intelligence Analysis Unit and the Courts.

Malta has transposed the Directive by virtue of Legal Notice 168 of 2018 entitled "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 Legal Notice entered into force on 28th May 2018.

2.3 Convention 108 and Convention 108+

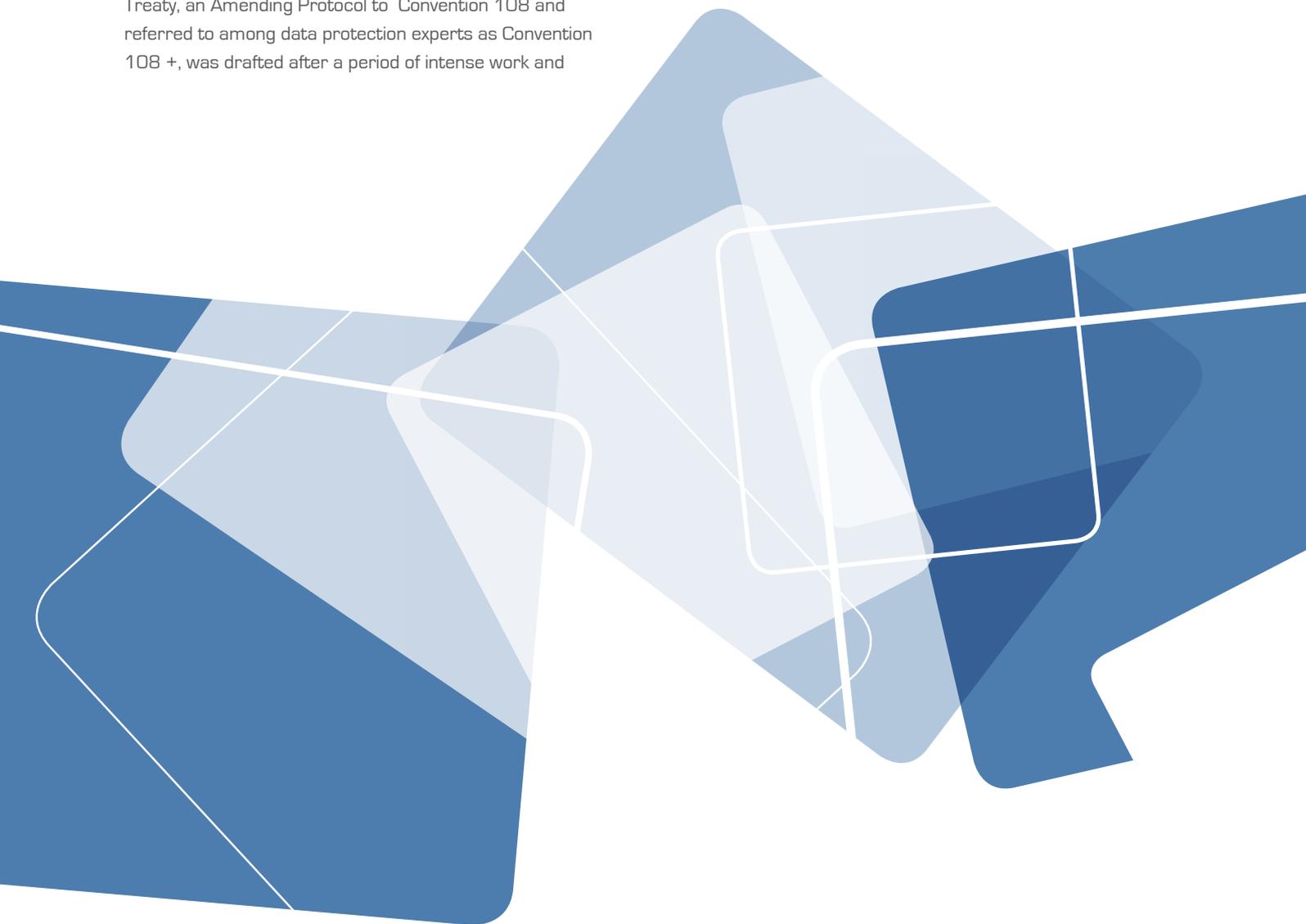
Convention 108 of the Council of Europe on the protection of individuals with regard to Automatic Processing of Personal Data is the first legally binding international instrument which protects the individual against abuses which may accompany the collection and processing of personal data and which seeks to regulate at the same time, the trans frontier flow of personal data. In this regard and in terms of this Convention all parties (including Malta) were required to take the necessary steps in their domestic legislation to apply the principles it lays down, in order to ensure respect in their territory for the fundamental human rights of all individuals with regard to processing of personal data. The Government of Malta ratified this Convention in 2003.

While the core principles contained in Convention 108 have undeniably stood the test of time the Council of Europe considered it necessary nonetheless to modernise this landmark instrument. With this in mind, a Council of Europe Treaty, an Amending Protocol to Convention 108 and referred to among data protection experts as Convention 108 +, was drafted after a period of intense work and

negotiations. Modernisation proposals were elaborated by the Committee of Convention 108 (T-PD) and reviewed between 2013 and 2016 by an Ad hoc Committee on data protection (CAHDATA), which in both committees, Malta is an active member.

It is imperative to mention that the revised text aims to ensure consistency, compatibility and harmonisation with other data protection legal frameworks, namely and in particular the GDPR.

The protocol opened for signatures on the 10th October 2018. Malta will eventually be one of the signatories.



3

Public
Awareness



3

Public Awareness

3.1 Activities

One of the functions of the Commissioner is to bring to the knowledge of the general public the provisions of the General Data Protection Regulation as complemented by national data protection law, and ultimately promulgate data protection awareness for the benefit of the citizens and also controllers operating within different sectors. This year was particularly intensive on such front, especially with the advent of the GDPR.

3.1.1 Presentations

The Commissioner engaged proactively with the relevant stakeholders, including constituted bodies in order to promulgate awareness on the new regulation to a wide audience. In addition, various requests for meetings and presentations were also accommodated even on an individual basis, to ensure that a general level of awareness is imparted across the board.

During the year under review, a total of 25 presentations were delivered either as part of dedicated information sessions or participation in conferences or seminars on data protection. These presentations were aimed at various stakeholders, including the following:

- Legal professionals
- ICT professionals
- The Judiciary
- Engineers
- Accountants
- SMEs
- Data Protection Officers
- Retailers and Sole Traders
- Trade Unions
- Employers
- Academics (University lecturers and staff)
- Students (post-secondary)
- Hoteliers and security personnel within hotels
- Financial services professionals
- Online gaming professionals

3.1.2 Discussions with Data Controllers

Apart from convening 520 one-to-one meetings with controllers, this Office also imparted advice through

conference calls in those cases where one-to-one meetings were not possible given the busy schedule especially prior to the coming into effect of the GDPR. In total, 35 scheduled conference calls were held with different controllers in order to answer specific questions on the new regulation.

3.1.3 Local TV, Radio and other media

During 2018, the Commissioner participated in local TV programmes and gave numerous interviews and contributions to TV, radio and newspapers. Furthermore, as in previous years, the Office participated in a monthly radio programme on data protection with live phone-ins. Such programme allows individuals to interact with representatives from the Office and discuss specific data protection concerns. Positive feedback has been registered from these awareness initiatives.

3.1.4 IDPC Website

Furthermore, the Office's portal has been revamped with dedicated sections concerning the GDPR, including information, updated legislative instruments and quick links to the relevant opinions issued by the EDPB. In addition, specific sections are intended to guide controllers to notify data breaches and conduct data protection impact assessments. Apart from these sections, information on complaints, press releases, latest news and other issues are regularly posted. The Office firmly believes that getting the message across various media, represents an effective manner to reach a wide audience and increase awareness with the public at large.

3.2 Data Protection Day

On 28 January 2018, the Data Protection Commissioner joined other Data Protection authorities across the globe to celebrate Data Protection Day in order to promote and raise awareness on privacy and data protection best practices. This date corresponds to the anniversary of the opening for signature in 1981 of the Council of Europe's Convention 108.

In the year under review the main activity planned, was the address and participation of the Information and Data Protection Commissioner together with the Parliamentary

Secretary for Consumer protection and Valletta 2018 within MJCL, in a seminar on data protection organised by the Data Protection Unit (MJCL), for Heads of Departments, Data Protection Officers and Directors within the Public Administration. Another activity was the delivery of a presentation to an association of IT professionals, as an awareness raising activity, at a GDPR Information Session. Other activities included the participation in a local, educational, radio programme with phone-ins highlighting developments occurring in the field of data protection.

3.3 Drafting of guidelines together with various sectors

As part of his functions, the Commissioner regularly engages in discussions with different stakeholders and associations or constituted bodies representing specific sectors. Where the nature of processing operations carried out by these sectors requires ongoing discussions, this Office normally establishes a working group, which serves as a forum for representatives from such sector or their association to bring up any data protection matter for discussion. The end result of these discussions is the issuing of guidelines or specific interpretations of data protection law in relation to the relevant sector.

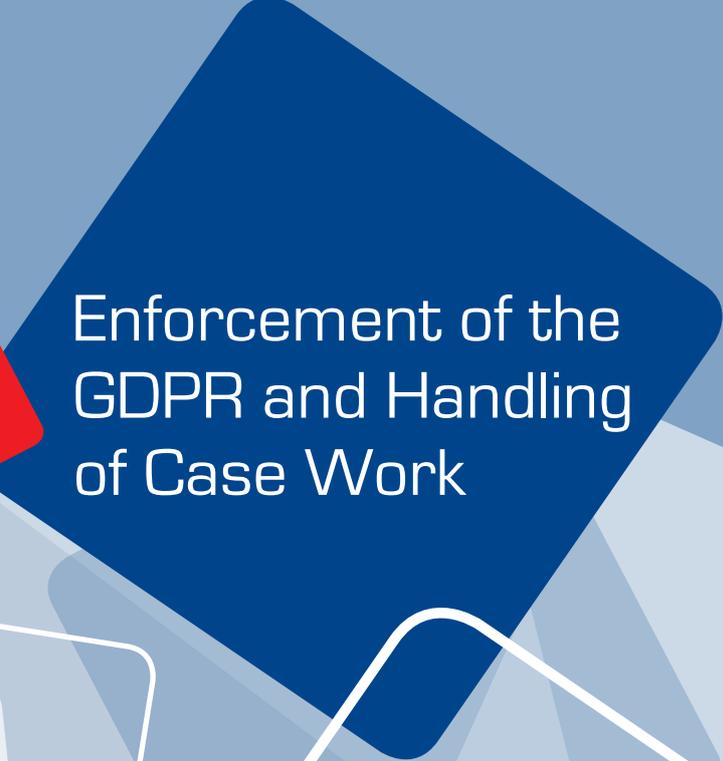
During the year under review, this Office experienced additional stakeholder engagement, mainly in view of the GDPR and the need for sectoral guidance in order to

facilitate a smooth transition and implementation of the new framework. Specific guidelines were issued for the banking and online gaming sectors in conjunction with the Malta Bankers Association and the Malta Gaming Authority respectively. These guidelines which were issued prior to the coming into effect of the GDPR, were the result of several meetings held with such bodies.

With the implementation of the GDPR, this Office continued to engage with the various stakeholders in order to discuss sector-specific issues. However, due attention is given to the provisions of Article 40 of the GDPR, laying down the procedure for the approval of codes of conduct. In its engagement with stakeholders, this Office clearly explains the implications of such Article, including the consistency mechanism which would be triggered where the processing covered by such code would affect several Member States.



4



Enforcement of the
GDPR and Handling
of Case Work



4

Enforcement of the GDPR and Handling of Case Work

The powers and tasks of the Commissioner are laid down under Articles 57 and 58 of the GDPR.

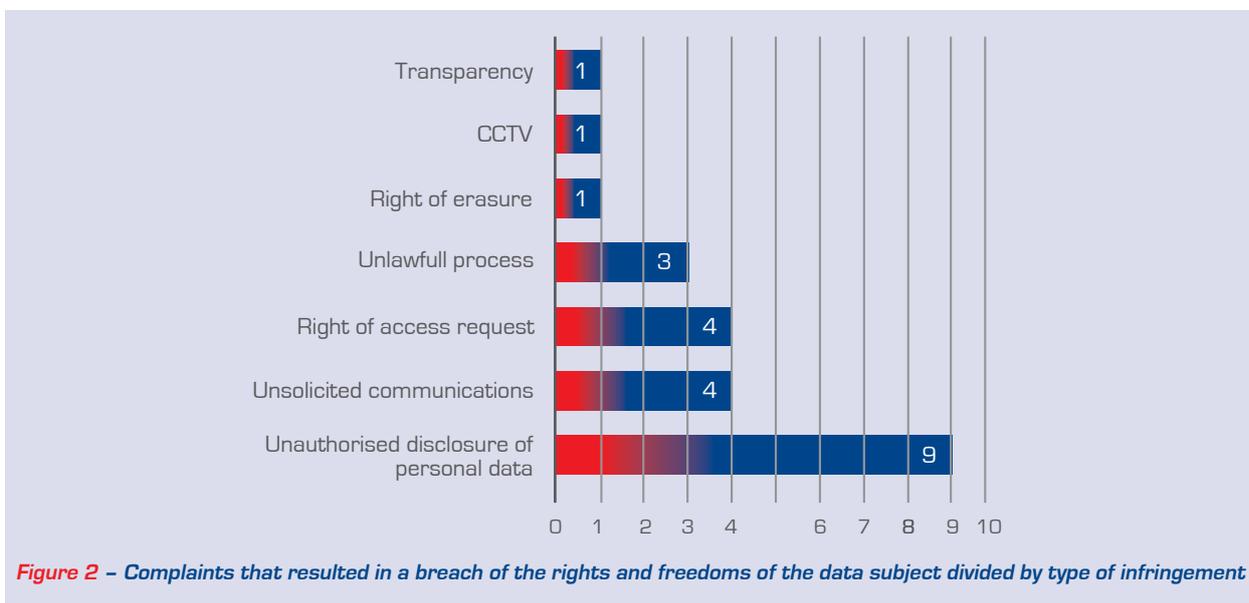
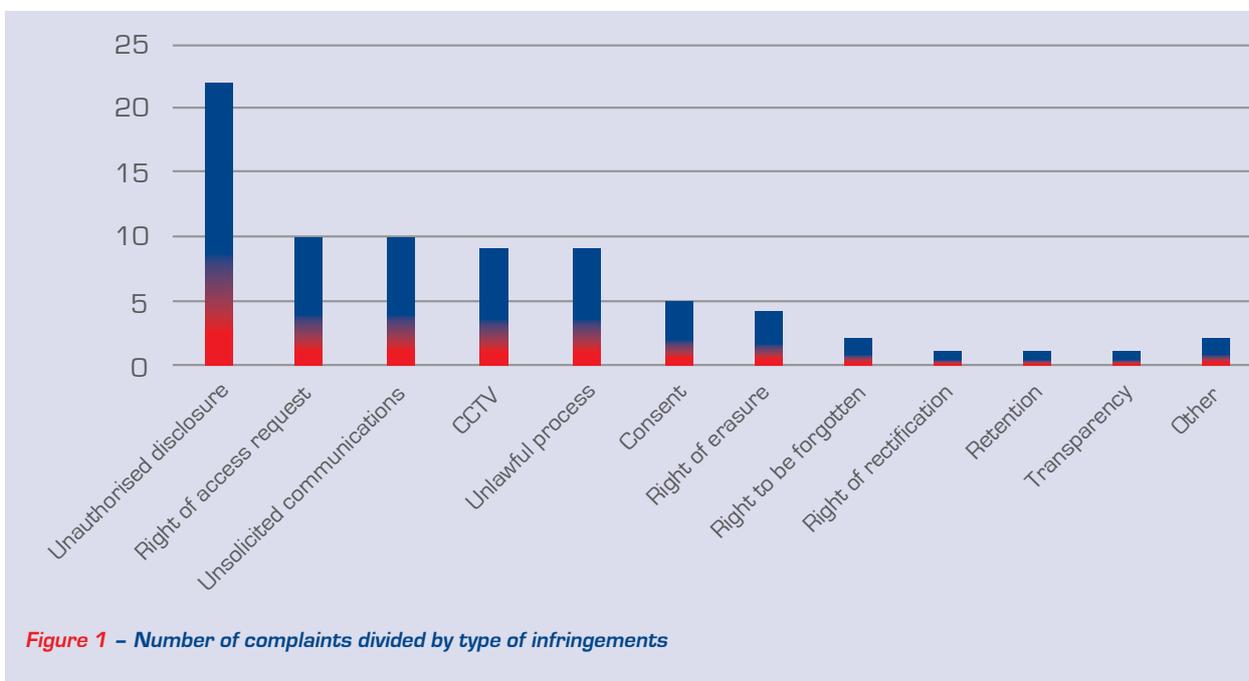
The Commissioner's complaint handling procedure involves a preliminary assessment to establish the admissibility of the cases. In the event that the case is considered not admissible, it is not investigated.

4.1 Handling of complaints with a national impact

In terms of Article 57(f) of the GDPR the Commissioner shall on its territory handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 80, and investigate, to the extent appropriate, the subject matter of the complaint.

In 2018, the Commissioner has investigated 76 data subject complaints.

In terms of Article 80 of the GDPR, the data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in



accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law.

All the complaints received by the IDPC in 2018 were filed by the data subjects themselves.

The below chart represents the complaints that have been investigated divided by infringements.

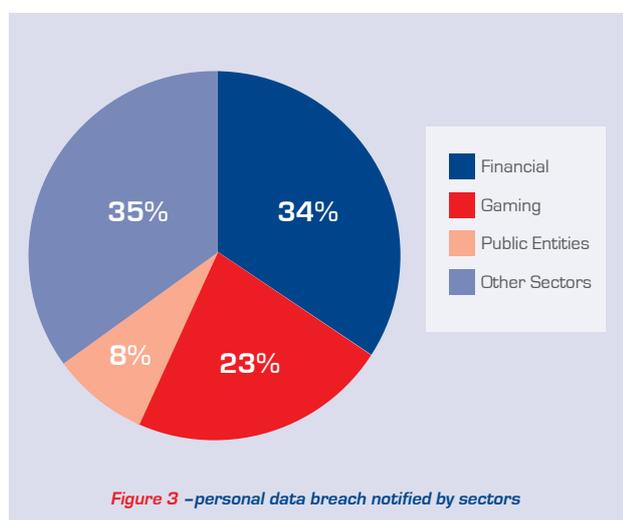
From the investigations it transpired that the data subjects' rights and freedoms were breached in 25 cases. The next chart shows these 25 cases divided by type of infringement.

4.2 Personal Data Breaches

In terms of Article 4(12) of the GDPR a personal data breach is 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.

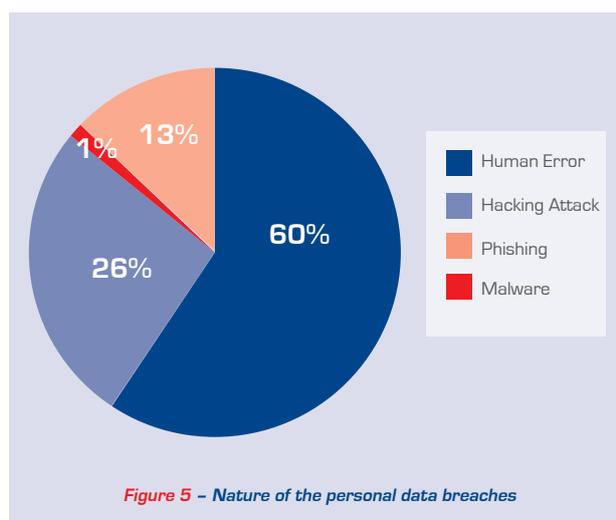
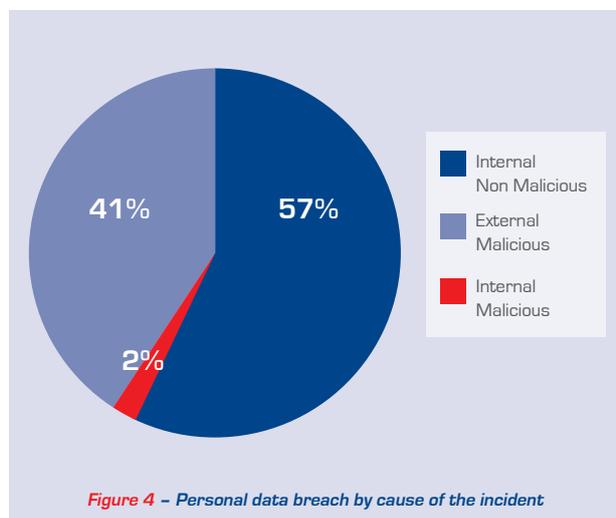
Article 33 of the Regulation set out an obligation for Data Controller to notify the personal data breach to the supervisory authority competent within 72 hours unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

The Office has developed and implemented an internal severity scoring tool to classify the breach notifications. This tool allows to determine the severity of the incident and helps to prioritize the investigation activities by considering some core parameters such as, but not limited to, type of



personal data breached, number of data subjects concerned, nature of the incident and consequences of the breach.

In 2018 this Office has received a total of 113 breach notifications. All the breaches were assessed and based on the outcome were investigated.



The chart (Figure 3) indicated the data breaches notified to this Office by sector.

In 2018 the two main causes of personal data breaches were human errors that, in most of the cases could be classified as not malicious, and external attacks such as hacking, phishing and malware.

The following two charts (Figure 4 and Figure 5) show the main causes and the nature of personal data breaches.

4.3 Enforcement action

Following complaints and data breaches the Commissioner took the following corrective action.

4.3.1 Administrative fines

The Commissioner has the power to impose administrative fines both on the private and the public sectors. Where the Commissioner imposes a fine, he shall by order in writing require the controller or processor, as the case may be, to pay such administrative fine, which shall be due to the Commissioner as a civil debt.

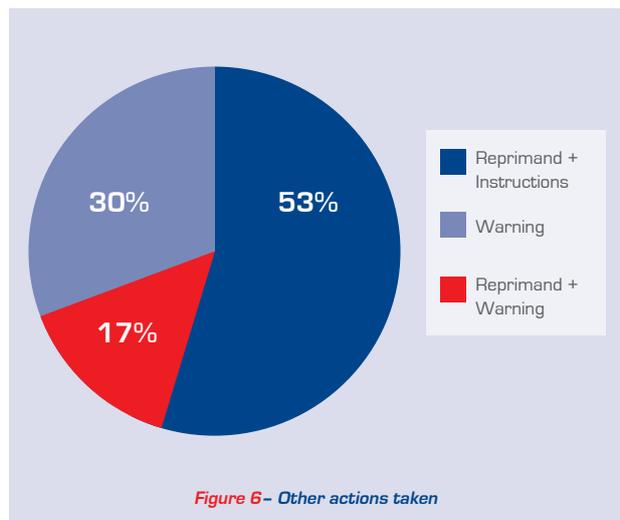
During the year under review the Commissioner imposed in total 18 fines, for a total amount of €20,500.

Several fines were imposed due to the repetitiveness of the incidents even if the severity of the potential impact on the data subject was low or medium.

4.3.2 Other action taken

In terms of Article 58(2)(a)(b)(d) each supervisory authority has also the power to issue reprimands, warnings and/or instructions to data controllers.

The following chart (Figure 6) represents which other actions were taken by the Commissioner in 2018 pursuant to Article 58.

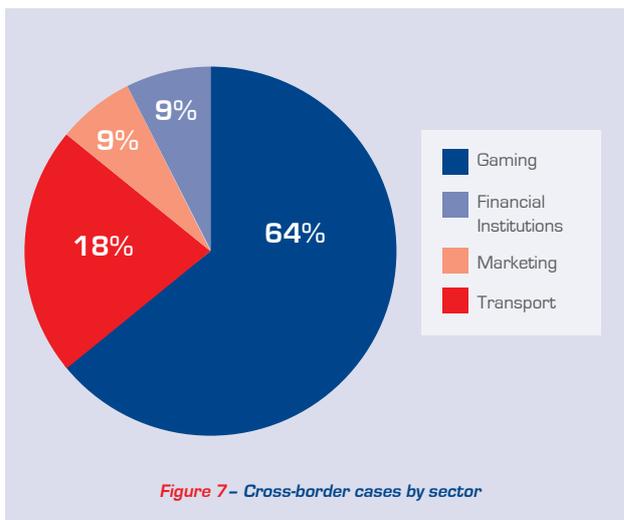


processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

Pursuant to this Article in cases of cross-border processing the supervisory authority in the territory of the main establishment of the data controller is the lead supervisory authority (LSA) for monitoring and ensuring compliance with the Regulation while the supervisory authorities in other countries where that controller is established, or where data subjects are substantially affected, or authorities to whom a complaint has been made, are referred to as concerned supervisory authorities (CSA). In terms of Article 60 of the GDPR the LSA is to cooperate with the other CSAs and exchange all relevant information with each other as necessary.

In 2018 this Office was identified as LSA in 12 cross-border cases. All the cases were dealt with in 2018 except 1 that was closed in October 2019.

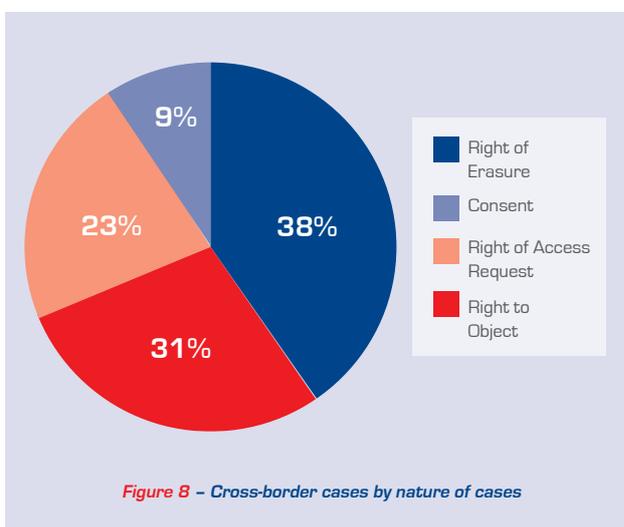
The chart below (Figure 7) indicates the sectors involved in cross-border cases.



It has to be noted that more than one power may be exercised for the same incident.

4.4 Cross Border Cases

Article 4(23) of the GDPR defines the cross-border processing as either: (a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or (b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or



The chart (Figure 9) takes into consideration the nature of the cross-border cases where the IDPC was considered as LSA.

4.4.1 Appeals

Chapter 586 – Data Protection Act – of the Laws of Malta, Article 26, establishes that any person to whom a legally binding decision of the Commissioner is addressed, shall have the right to appeal in writing to the Tribunal within twenty days from the service of the said decision as provided in article 23 of the same act.

There were only 3 decisions out of 86 decisions which were appealed before the Appeal Tribunal in 2018. Out of these 3 decisions, 2 were referred to the Court of Appeal.





5

European and
International
Activities



5

European and International Activities

As part of his role, the Commissioner honoured his European and International commitments, involving participation in the main data protection conferences, meetings and fora. These platforms are not only useful to discuss specific or common issues and enhance the level of cooperation with other DPA's, but also serve as an invaluable source of knowledge sharing.

5.1 European Data Protection Board (EDPB)

On the 25th of May 2018, the day when the GDPR became enforceable, the newly set up European Data Protection Board (EDPB) started to exercise its functions established under such Regulation, taking over the work and legacy from its predecessor, the Article 29 Working Party established under the previous Data Protection Directive (EU 95/46). The EDPB is an independent European body established under the GDPR with a legal personality. The main role of the EDPB is to contribute to the consistent application of data protection rules throughout the European Union and promote cooperation between supervisory authorities. The EDPB is composed of the heads of the Supervisory Authorities and the European Data Protection Supervisor (EDPS) or their representatives. The Commissioner is an active member of the EDPB.

Between 25 May and 31 December 2018, the EDPB held five plenary sessions, apart from the expert subgroups operating under its structure, where 36 meetings were held. At its first meeting the EDPB endorsed 16 Guidelines previously issued by the Article 29 Working Party. During the remainder of 2018, the EDPB adopted four more Guidelines aimed at clarifying a range of provisions under the GDPR. In particular, these Guidelines addressed certification and the identification of certification criteria, derogations relating to international transfers, the territorial scope of the GDPR and the accreditation of certification bodies.

During such period, the EDPB reviewed and adopted 26 Opinions on the national lists of processing operations subject to a Data Protection Impact Assessment (DPIA). The purpose of the exercise was to ensure consistency across all national lists. These Opinions included the national list for Malta which was adopted in 16th October 2018. Such list can be found on the IDPC website.

The EDPB also advises the European Commission on any issue related to the protection of personal data, including assessments of the standard of data protection in third countries or international organisations. In 2018, the EDPB issued two such Opinions, at the request of the Commission: one on electronic evidence (e-Evidence) and one on the EU-Japan draft adequacy decision.

5.2 EDPB - Expert Sub-groups

Apart from the involvement in the EDPB, the Commissioner also assigns members of his staff to closely follow the developments and contribute as far as possible, to selected expert sub-groups which are deemed highly relevant and impactful to the work conducted at the Office. Currently, four expert sub-groups are being attended, while other sub-groups, depending on the agenda items which are considered of interest, are occasionally followed through the video-conference facilities.

5.2.1 Borders, Travel and Law Enforcement Subgroup (BTLE)

The BTLE is a subgroup established under the structure of the EDPB and tasked with EU data protection matters concerning borders, travel and law enforcement. The subgroup consists of representatives from data protection authorities including our Office. Its work programme is subject to a mandate given by the supervisory authorities in the board and its work activities are reported to the EDPB plenary. The BTLE meets approximately (5) times a year usually a fortnight before the plenary meeting.

During 2018, major discussions related to the following:

- EU-US Privacy Shield and the joint review;
- EDPB Guidelines on the interpretation of Article 47 of the Law Enforcement Directive concerning the powers of Supervisory Authorities;
- Article 48 of the GDPR and its relation to the US Cloud Act (and the Microsoft Warrant Case);
- Passenger Data (PNR) – regular updates were provided by the Commission;
- Future of supervision models for EU large IT systems in the JHA area;
- Adequacy Decision on Japan;
- EU proposal on E-evidence; and
- Interoperability proposals.

5.2.2 Technology expert sub-group

This Office regularly participates in this expert group, which, during the year under review, particularly following the coming into application of the GDPR, increased the frequency from once every quarter to once every month. The meeting is generally spread over 1 or 2 days, depending on the items on the agenda. The expert group mostly discusses subject areas that are technological in nature and develops guidelines according to the annual work plan and mandates given by the European Data Protection Board. The topics that were discussed during the year under review included certification and accreditation, data breach notifications, connected vehicles, DPIA lists, video surveillance and data protection by design and default.

5.2.3 IT Users subgroup

The EDPB has a number of IT tools to facilitate the cooperation mechanism and the sharing of information between data protection authorities. Since the implementation of these systems the IDPC has a representative attending in the IT Users subgroup to remain updated on the continuous developments and to share its experience as user with the other participants.

5.2.4 Fining Task Force

The IDPC attended the Fining Task Force since the first meeting. The aim of the Fining Task Force is the sharing of experiences in imposing fines pursuant to Article 83 of the GDPR with a view of developing guidelines on the harmonisation of the calculation of fines and in order to observe the consistency in enforcement action involving administrative fines.

5.3 International Conference

The International Conference of Data Protection and Privacy Commissioners (ICDPPC) is a worldwide annual forum at which independent regulators on privacy and data protection adopt high level resolutions and recommendations addressed to governments and international organisations. The Conference first met in 1979 and for almost four decades now, it has provided international leadership to data protection and privacy. It connects the efforts of 115 privacy and data protection regulators from across the globe. The ICDPPC consists of a closed session and a public session. The closed session is attended by accredited members and observers; the public session is attended by these members and observers in addition to a wider audience from the data protection and privacy community, industry, civil society, academia and government representatives. As an accredited member of the Conference, the Commissioner participates both in closed and public sessions.

This year's Conference which marked the 40th edition, was held in Brussels between the 22nd and 26th October with side events also in Sofia. The theme of the Conference was "Debating ethics: dignity and respect in data driven life".

With the continued development of technologies using facial recognition, artificial intelligence, and genetic data, getting ethics decisions right is going to be even more essential.

To that end, a declaration on ethics and data protection in artificial intelligence was adopted during the Conference. Furthermore, additional resolutions were also presented on the following:

- E-learning platforms;
- ICDPPC rules and procedures;
- Future of the International Conference;
- Collaboration between Data Protection and Consumer Protection Authorities;
- Conference Census.

5.4 European Data Protection Conference

The Commissioner is also an accredited member of the conference of the European Data Protection Authorities, most commonly referred to as the Spring Conference. This year's Conference (the 28th edition) with the theme "Data Protection – Better Together", was held in Tirana on the 3rd and 4th of May.

The Conference consisted of different panels which included contributions from Commissioners and officials from data protection authorities, as well as other exponents from the data protection community.

5.5 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. Two meetings were convened in 2018.

5.6 Joint Supervisory Body of Eurojust

The Joint Supervisory Body (JSB) of Eurojust is an independent external supervisor in the field of data

protection, which collectively monitors Eurojust's activities involving the processing of personal data and ensures that they are carried out in accordance with the Eurojust Decision. The members of the JSB are judges or persons with an equal level of independence (in practice data protection commissioners) and therefore have substantial expertise both in the fields of data protection and judicial co-operation.

During the year under review the office gave its contribution to this European forum by participating in its annual meeting of national experts with a focus on enhancing the use of joint investigation with faster, simpler and more effective processes.

5.7 Schengen Information System II Supervision Coordination Group (SIS II SCG)

The Schengen Information System allows competent authorities of participating Member States to obtain information regarding certain categories of persons and objects.

The system establishes communication amongst all Member States and provides end-users with access to information in accordance with the applicable legal framework. It is a vital factor in the smooth running of the area of security, freedom and justice. It contributes to the implementation of the provisions on the free movement of persons and to judicial cooperation in criminal matters and police cooperation. Given the amount and nature of personal data being processed in the system, and also the negative impact it can have on individuals, effective supervision, both centrally and on a national level is essential.

The SIS II SCG is a platform in which the data protection authorities responsible for the supervision of SIS II, according to Article 46 of the SIS II Regulation and Article 62 of the SIS II Decision cooperate in the framework of their responsibilities in order to ensure a coordinated supervision of SIS II. The Coordination Group is composed of representatives from the national data protection authorities supported by a secretariat which is provided by the European Data Protection Supervisor.

The IDPC representative has been elected chair of this working group since 2017. This is clearly an accomplishment for a small Data Protection Authority like ours and proves recognition at the European level. At the same time, it demands hard work and commitment.

During the last year, the group continued its work in line with the activities as predefined in its work programme. In particular, the group focused on the following:

- Logging procedures at national level;
- Legislative developments including the interoperability proposals;
- Update of the SIS II Right of Access guide;
- National criteria for raising Article 24 alerts;
- The increase in Article 36 alerts; and
- SIS II SCG Website.

Apart from the abovementioned items, regular discussions on Schengen matters were held both with the Data Protection Officer of eu-LISA and also representatives from the Commission, who are invited to provide updates during each meeting.

5.8 Visa Information System Supervision Coordination Group (VIS SCG)

The Visa Information System (VIS) is established under Regulation 2008/767EC 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. To this end, the VIS provides a central repository of data on all short-stay Schengen visa. This data can be accessed by authorities issuing visas such as consulates of Member States, by checkpoints at the Schengen border to verify the identity of visa holders, as well as for the purpose of identifying third-country nationals apprehended within the Schengen Area with fraudulent or without documents. Supervision over the national units is allocated to the DPAs in the respective Member State, while the central VIS is supervised by the EDPS.

For such purposes, the VIS Supervision Coordination Group (VIS SCG) has been set up and meets twice a year. The VIS SCG is composed of representatives from the national DPAs and the EDPS.

5.9 Eurodac Supervision Coordination Group (Eurodac SCG)

Eurodac is an information system set up for the purpose of identifying the Member State responsible for an asylum application lodged within the European Union, and in order to speed up the asylum procedure. The system enables the identification of asylum seekers and persons who have illegally crossed an external border of the European Union. The system allows Member States, through comparison of fingerprints, to verify whether an asylum seeker or foreign national, found irregularly present within the community has previously claimed asylum in another Member State, thus combating asylum shop around.

Eurodac Supervision is carried out centrally, by the EDPS, who is the competent authority to monitor the Central Unit, while at the national level, the data protection authorities (DPAs) of each participating state are responsible to oversee the collection, use and transmission of data occurring in their country.

In the framework of coordinated supervision, the EDPS and DPAs meet under the Eurodac SCG platform at least twice a year to discuss common issues relating to the supervision of the data processing in Eurodac.

Major activities carried out by the Eurodac SCG during 2018 were the survey on data subjects' rights, advance erasure of data in the system, the use of special searches, and also discussions on possible collaboration with the Fundamental Rights Agency (FRA), in coming up with information material on the rights of data subjects.

5.10 Customs Supervision

The Customs Information System (CIS) is an information system which centralises customs information, allowing for a more efficient detecting and prosecuting of violations of customs and agricultural matters. With the CIS, national customs administrations can exchange information about illegal trafficking and intervention requests. The purpose of the CIS is to prevent, investigate and prosecute serious violations of national legislations by making the cooperation and oversight procedures of the customs administrations of Member States more efficient.

The CIS operates with two separate databases: one relates to actions taken by the European Community and the other relates to intergovernmental actions.

In 2018, the group mainly focused on developing a common format for inspecting CIS, including a common inspection plan for AFIS security policy. In addition, the group also pursued its work on the guide for exercising the right of access to CIS.

5.11 Council of Europe Consultative committee (T-PD)

Malta, being a party to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention ETS no.108), is a member of the consultative committee (T-PD) set up in terms of Chapter V of the Convention, which meets regularly in January and June, and is entrusted inter alia to make proposals to facilitate or improve the application of the convention and to suggest amendments to the convention. During the year under review the office gave its contribution to this international forum by participating in its plenary meetings which focused on personal data in the police sector, safeguarding privacy in the media and artificial intelligence, among others.



6

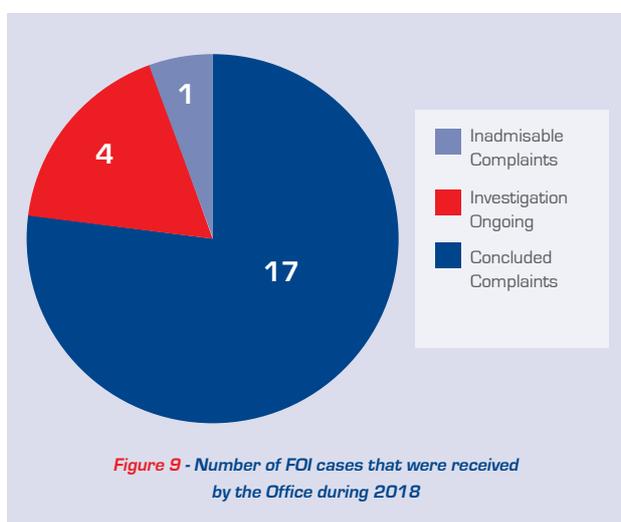
Freedom of
Information



6

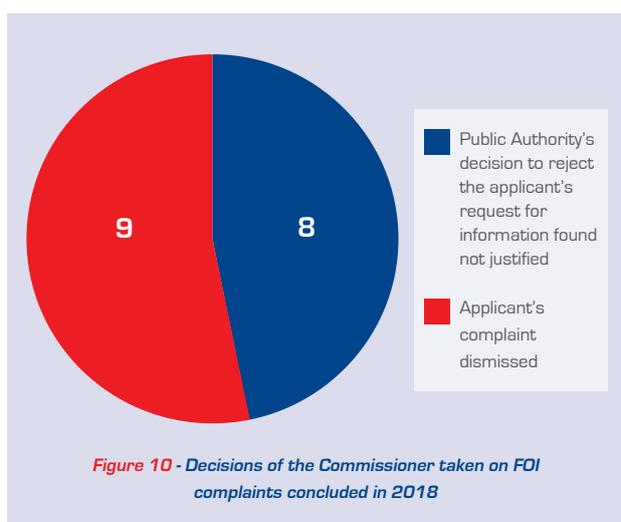
Freedom of Information

As part of its regulatory functions, this Office is also responsible for the enforcement of the freedom of information legislation. During the year under review, 22 complaints were received from applicants, mainly journalists, who were not satisfied with the decisions taken by the public authorities on their requests for information.



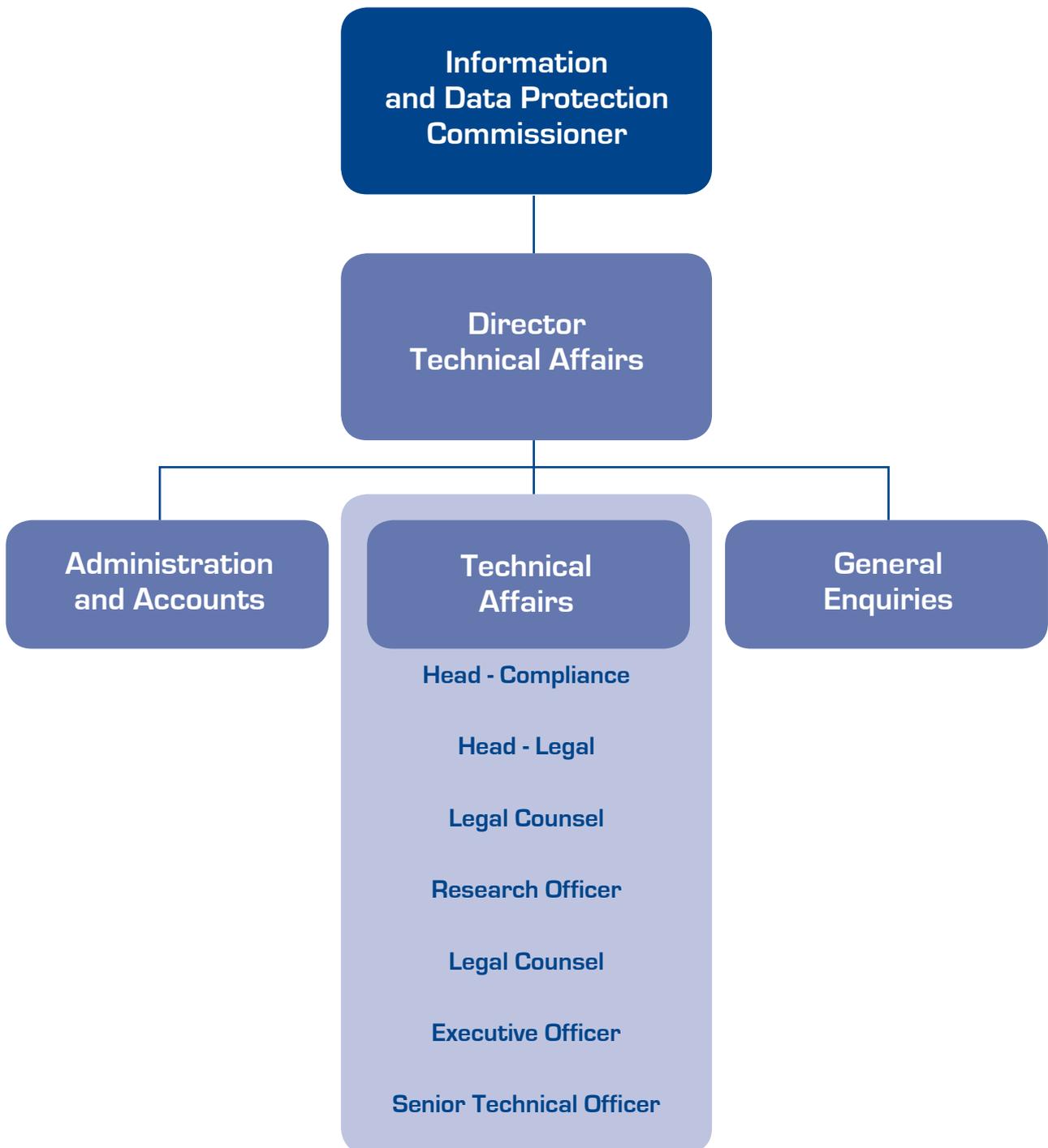
As represented in the previous 2 figures, during the year under review, the Commissioner initiated an investigation on all the 21 complaints received and issued an official decision on 17 cases. In 8 of the cases, the Commissioner found in favour of the applicant and instructed the Public Authority to provide him with the requested document. The other 4 complaints which are still subject to an ongoing investigation, are expected to be concluded in the first half of 2019.

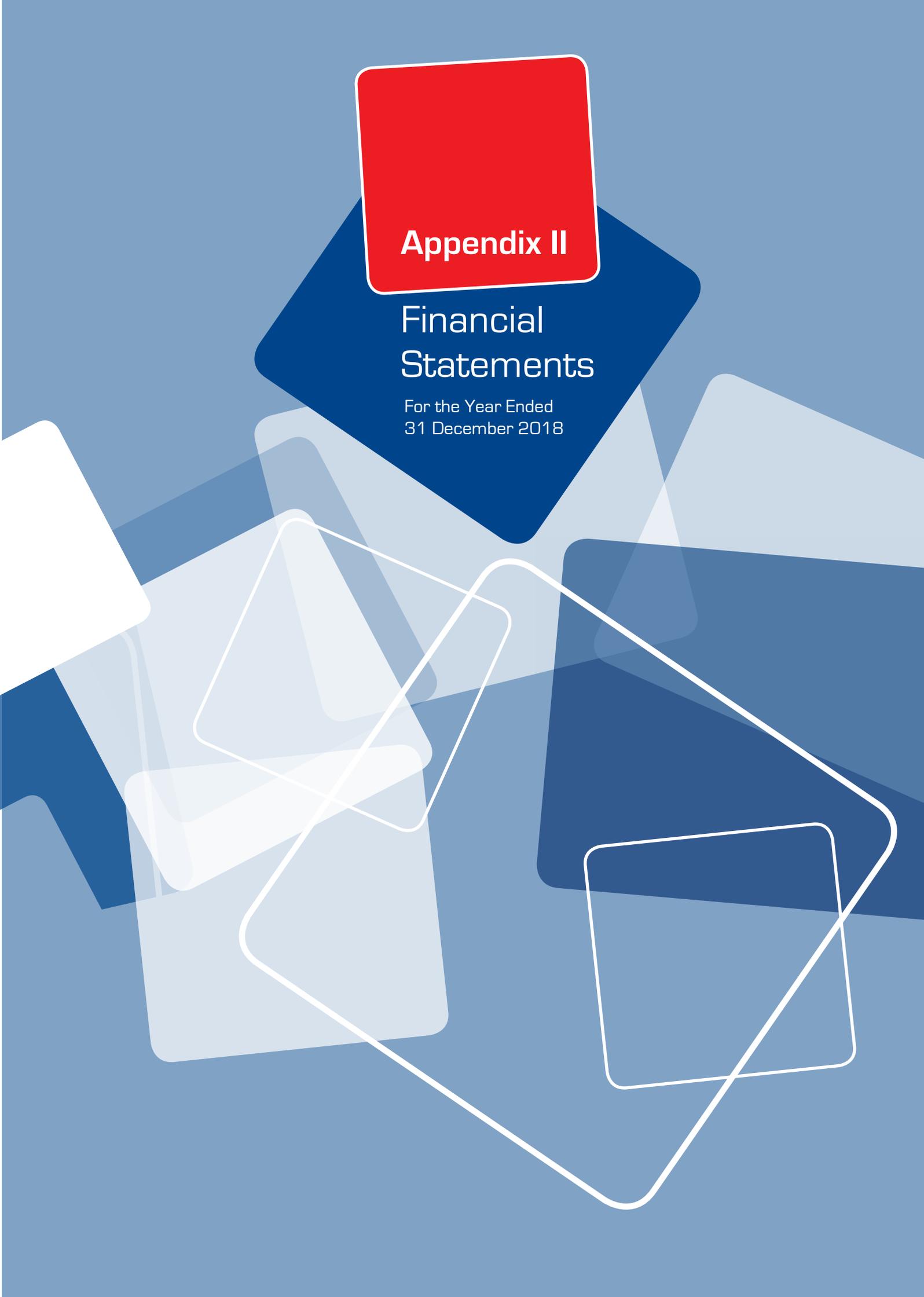
Out of the 17 concluded cases, 5 of the Commissioner's decisions were appealed before the Information and Data Protection Appeal Tribunal where one of the parties felt aggrieved by such decision and exercised his right at law to seek judicial redress. Another case was filed before the Tribunal by a Public Authority who appealed an Information Notice issued by the Commissioner pursuant to Article 24 of the Freedom of Information Act. This notice is served on public authorities during the initial stages of the investigation procedure where, the Commissioner exercises his power to collect the necessary information, including but not limited to, the document that would have been requested by the applicant, for the purposes of establishing all the facts on the complaint and be able to make the necessary legal considerations during the decision making process.



The appeals filed with the Tribunal during the year under review are awaiting judgment.

Appendix I Organisation Chart



The cover page features a dark blue background with several overlapping, semi-transparent geometric shapes in various shades of blue and white. A prominent red rounded square is positioned at the top center. The text is centered and uses a clean, sans-serif font. The overall design is modern and professional.

Appendix II

**Financial
Statements**

For the Year Ended
31 December 2018



Commissioner's Report

For the Year Ended 31 December 2018



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 2018.

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 closed the year with a surplus of €35,352 (2017: €251) before taking into account the result from the collection of notification fees. The Office received Government subvention amounting to €450,000 in 2018, representing an increase of 12.5% compared to 2017. Total administrative expenditure incurred amounts to €414,683, resulting in an increase of 3.7% compared to 2017. 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 is still in force as at today. In 2018, the Office has incurred an overall loss of €7,445 from the collection of notification fees, when taking into consideration the upward movement in the provision of doubtful debts by €98,133.

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

Events after the balance sheet date and future developments

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

Commissioner

The present Commissioner who held office during the year was **Mr. Saviour Cachia**.

The present Commissioner shall continue in office.



Statement of the Commissioner's responsibilities for the financial statements

For the Year Ended 31 December 2018

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;
- 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), Certified Public Accountants and Registered Auditors, have expressed their willingness to continue in office and a resolution for their reappointment will be proposed at the Annual General Meeting.

Approved by the Commissioner on 03 May 2019 and signed on its behalf by:

Mr. Saviour Cachia
Commissioner

Registered Address:

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

Independent Audit Report

For the Year Ended 31 December 2018



We have audited the accompanying financial statements of the Office of the Information and Data Protection Commissioner set out on pages 5 to 15 which comprise the statement of financial position as at 31 December 2018, 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.

Qualified Opinion

In our opinion, except for the effects of the matter described in the Basis for Qualified Opinion section of our report, the accompanying financial statements present fairly, in all material respects, the financial position of the Office as at 31 December 2018, and its financial performance for the year then ended in accordance with International Financial Reporting Standards as adopted by the European Union.

Basis for Qualified Opinion

On the 25 May 2018, the General Data Protection Regulation (GDPR) has been enacted. As a result of this new regulation, there is no longer an obligation on individuals and body of persons to pay an annual notification fee to the Office. Using an accounting package, The Office recorded notification fees based on manual applications submitted by controllers, as in terms of Article 29 of the Data Protection Act, Chapter 440, “the controller shall notify the Commissioner before carrying out any wholly or partially automated or manual processing operation or set of such operations intended to serve a single purpose or several related purposes”. The notification fees are immediately passed to the Central Government when collected by the Office. As a result of this system, we were unable to confirm or verify by alternative means the accounts receivable included in the statement of financial position which is fully provided for as at 31 December 2018. As a result of these matters, we were unable to determine whether any adjustments might have been found necessary in respect of recorded or unrecorded accounts receivable, and, the consequential adjustments, if any, arising out of these are not quantifiable.

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 qualified opinion.

Other Information

The Commissioner is responsible for the other information. The other information comprises the Commissioner’s report. 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.

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.



Mr. George Mangion

for and on behalf of
PKF (Malta)

Certified Public Accountants and Registered Auditors

03 May 2019

Statement of Comprehensive Income

For the Year Ended 31 December 2018



	Note	2018 €	2017 €
Government subvention		450,000	400,000
Administrative expenses		(414,683)	(399,749)
Other income		35	-
Surplus for the year	4	35,352	251
Result from collection of notification fees	3	(7,445)	(90,787)
Total result transferred to retained funds		27,907	(90,536)

The notes on pages 9 to 15 form an integral part of these financial statements.

Statement of Financial Position

As at 31 December 2018



	Note	2018 €	2017 €
ASSETS			
Non-current assets			
Property, plant and equipment	7	15,004	11,614
Intangible assets	8	-	-
Total non-current assets		15,004	11,614
Current assets			
Trade and other receivables	9	7,922	129,169
Cash and cash equivalents	10	90,536	55,930
Total current assets		98,458	185,099
TOTAL ASSETS		113,462	196,713
EQUITY AND LIABILITIES			
Equity			
Retained Funds		83,020	55,113
Total equity		83,020	55,113
Liabilities			
Current liabilities			
Trade and other payables	11	30,442	141,600
Total current liabilities		30,442	141,600
TOTAL EQUITY AND LIABILITIES		113,462	196,713

The notes on pages 9 to 15 form an integral part of these financial statements.

These financial statements on pages 5 to 15 were approved by the Commissioner on 03 May 2019 and were signed by:

Mr. Saviour Cachia
Commissioner

Statement of Changes in Equity

For the Year Ended 31 December 2018



	Retained Funds €	Total Equity €
Balance as at 01 January 2018	55,113	55,113
Profit for the year - total comprehensive income	27,907	27,907
Balance as at 31 December 2018	83,020	83,020
Balance as at 01 January 2017	145,649	145,649
Loss for the year - total comprehensive income	(90,536)	(90,536)
Balance at 31 December 2017	55,113	55,113

The notes on pages 9 to 15 form an integral part of these financial statements.

Statement of Cash Flows

For the Year Ended 31 December 2018



	Note	2018 €	2017 €
Cash from operating activities:			
Profit from operations		27,907	(90,536)
Other increases (decreases) to reconcile to profit (loss) from operations		-	1,795
Depreciation		6,650	6,562
Provision for doubtful debts		-	27,383
Profit/(loss) from operations		34,557	(54,796)
Movement in trade and other receivables		121,248	78,260
Movement in trade and other payables		(111,159)	38,156
Net cash flows from operating activities		44,646	61,620
Cash flows from investing activities:			
Payments to acquire property, plant and equipment		(10,040)	(1,253)
Net cash flows used in investing activities		(10,040)	(1,253)
Net cash from in cash and cash equivalents		34,606	60,367
Cash and cash equivalents at beginning of year		55,930	(4,437)
Cash and cash equivalents at end of year	10	90,536	55,930

The notes on pages 9 to 15 form an integral part of these financial statements.

Notes to the Financial Statements

For the Year Ended 31 December 2018



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.

2. Significant Accounting Policies

a. Going concern

The financial statements has 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. 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.



2. Significant Accounting Policies (Continued)

b. Property, plant and equipment (Continued)

ii. Depreciation

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

Furniture and fixtures	10%
Motor vehicles	20%
Office equipment	15%
Computer software	25%
Air conditioners	25%

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

c. Intangible Assets

Intangible asset is stated at cost less accumulated amortisation and accumulated impairment losses. Intangible asset recognised in the Statement of Financial Position represents the cost of the new portal developed as part of the E-Government program in conjunction with the Ministry of Information Technology and Investments. Amortisation is recognised on a straight-line basis over the estimated useful life of the portal. The estimated useful life and amortisation method are reviewed at the end of each reporting period, with the effect of any changes in estimate being accounted for on a prospective basis. The intangible asset is amortised over the rate of 15%.

d. Financial assets and financial liabilities

A financial asset or a financial liability is recognised on the Office's Statement of Financial Position when the Office becomes a party to the contractual provisions of the instrument.

Financial assets and financial liabilities are initially recognised at their fair value plus transaction costs attributable to the acquisition or issue of the financial assets and financial liabilities.

Financial assets and financial liabilities are derecognised if and to the extent that, it is no longer probable that any future economic benefits associated with the item will flow to or from the entity.

A financial instrument, or its component parts, is classified as a financial liability or financial asset in accordance with the substance of the contractual arrangement rather than its legal form.

i. Other receivables

Other receivables are stated at their nominal value as reduced by appropriate allowances for estimated irrecoverable amounts. Trade receivables are assessed for impairment on a collective basis even if they were assessed not to be impaired individually. The management of the Office of the Information and Data Protection Commissioner resolved that a provision for doubtful debts is to be provided for any outstanding notification fees exceeding three years, in view that the recoverability of certain revenue may prove difficult and may consequently result in bad debts.



2. Significant Accounting Policies (Continued)

d. Financial assets and financial liabilities (Continued)

ii. Other payables

Other payables are stated at their nominal values.

e. Impairment

i. Financial assets

A financial asset is considered to be impaired if objective evidence indicates that one or more events have had a negative effect on the estimated future cash flows of that asset. An impairment loss in respect of a financial asset measured at amortised cost is calculated as the difference between its carrying amount, and the present value of the estimated future cash flows discounted at the original effective interest rate. An impairment loss in respect of an available-for-sale financial asset is calculated by reference to its current fair value.

Individually significant financial assets are tested for impairment on an individual basis. The remaining financial assets are assessed collectively in groups that share similar credit risk circumstances. All impairment losses are recognised in profit or loss. Any cumulative loss in respect of an available-for-sale financial asset recognised previously in equity is transferred to profit or loss.

An impairment loss is reversed if the reversal can be related objectively to an event occurring after the impairment loss was recognised. For financial assets measured at cost and available-for-sale financial assets that are debt securities, the reversal is recognised in profit or loss. For available-for-sale financial assets that are equity securities, the reversal is recognised directly in equity.

ii. 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. Cash and cash equivalents

i. 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.

Notes to the Financial Statements (continued)

For the Year Ended 31 December 2018



2. Significant Accounting Policies (Continued)

g. Income recognition

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.

Subventions from Government available to cover recurrent expenditure are reflected in the Statement of Comprehensive Income of the Office of the Information and Data Protection Commissioner on a receipt basis.

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

h. 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 or 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 value

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

3. Result from collection of notification fees

	2018	2017
	€	€
Revenue from Notifications	85,455	165,735
Income from Fines for Late Payment of Notification Fees	38,553	19,036
Reimbursement of Notification Fees to Government (note 1)	(33,320)	(248,175)
Provision for doubtful debts	(98,133)	(27,383)
Total	(7,445)	(90,787)

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.

Notes to the Financial Statements (continued)

For the Year Ended 31 December 2018



4. Surplus/(Deficit)

a. Surplus/(Deficit)

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

	2018	2017
	€	€
Auditors remuneration	2,065	2,065
Depreciation expense	6,650	6,562
Total	8,715	8,627

b. Auditors' remuneration

Total remuneration paid to the auditors during the year amounted to:

	2018	2017
	€	€
Audit Fees	2,065	2,065
Total	2,065	2,065

5. Taxation

The Commissioner as per previous practice, considers the Office is tax exempt and did not provide for tax at 35% in the financial statements. A request in terms of Article 12(2) of the Income Tax Act to obtain a tax exemption on its surplus will be made with the Ministry of Finance. To date, no such exemption has been received.

6. Wages and Salaries

a. Wages and salaries

Payroll costs for the year comprise of the following:

	2018	2017
	€	€
Gross Wages and Salaries	285,529	248,824
Social Security Contributions	19,440	16,501
Total	304,969	265,325

b. Average number of employees

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

	2018	2017
Commissioner	1	1
Directly Employed by the Office	8	7
Total	9	8

Notes to the Financial Statements (continued)

For the Year Ended 31 December 2018



7. Property, plant and equipment

	Furniture and fixtures €	Motor vehicles €	Office equipment €	Computer software €	Air conditioners €	Total €
Cost						
Opening balance	41,522	17,445	49,271	13,117	1,876	123,231
Additions	859	684	8,497	-	-	10,040
Disposals	-	-	-	-	-	-
Balance at 31 December 2018	42,381	18,129	57,768	13,117	1,876	133,271
Depreciation						
Opening balance	(38,255)	(13,920)	(44,325)	(13,241)	(1,876)	(111,617)
Depreciation	(556)	(3,480)	(2,738)	124	-	(6,650)
Disposals	-	-	-	-	-	-
Balance at 31 December 2018	(38,811)	(17,400)	(47,063)	(13,117)	(1,876)	(118,267)
Net Book Value						
At 31 December 2017	3,267	3,525	4,946	(124)	-	11,614
At 31 December 2018	3,570	729	10,705	-	-	15,004

8. Intangible Assets

E-Government Portal with a cost value of €29,932 is fully depreciated as at 31 December 2018.

9. Trade and other receivables

	2018 €	2017 €
Notification fee receivables	222,933	252,745
Provision for doubtful debts for notification fees	(222,933)	(124,800)
Prepayments	7,922	1,224
Total	7,922	129,169

10. Cash and cash equivalents

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

	2018 €	2017 €
Cash on hand	4	1,064
Bank balances	90,532	54,866
Total cash and cash equivalents	90,536	55,930
Total cash and cash equivalents in the statement of cash flows	90,536	55,930

Notes to the Financial Statements (continued)

For the Year Ended 31 December 2018



11. Trade and other payables

	2018	2017
	€	€
Creditors	26,642	13,923
Accruals	3,800	47,390
Deferred income from notifications	-	80,287
Total	30,442	141,600

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.

13. Comparative figures

Certain comparative figures have been reclassified to conform with the current year's financial statements presentation.

	2018	2017
	€	€
Administrative expenses		
Wages and Salaries	221,410	191,740
N.I. & Tax	83,559	73,585
Accountancy Fees	12,107	10,042
Auditors remuneration	2,065	2,065
Advertising Fees	1,547	1,326
Cleaning of premises	1,842	1,449
Consumables	2,843	2,373
Water and Electricity Fees	2,283	2,596
Car Hire Expenses	4,383	6,044
Insurance	307	403
Rent Expenses	25,000	25,000
Fuel Expenses	4,913	3,384
Legal Fees	(15)	1,667
Printing, Postage and Stationery Fees	4,817	13,195
Repairs and Maintenance Fees	1,414	4,158
Internet Subscription Fees	1,224	1,125
Telephone Fees	6,050	4,950
Travelling Fees	25,423	33,915
Parking Fees	3,610	2,724
Registration Fees	-	2,309
Hospitality Costs	140	759
General and Incidental Expenses	2,693	7,709
Bank charges	418	450
Depreciation and Amortisation	6,650	6,562
Other expenses	-	219
Total	414,683	399,749

Schedules do not form part of the audited financial statements.



Information and Data Protection Commissioner
Floor 2, Airways House, High Street
Sliema, SLM 1549, Malta.
Tel: (356) 2328 7100
E-mail: idpc.info@idpc.org.mt
www.idpc.org.mt