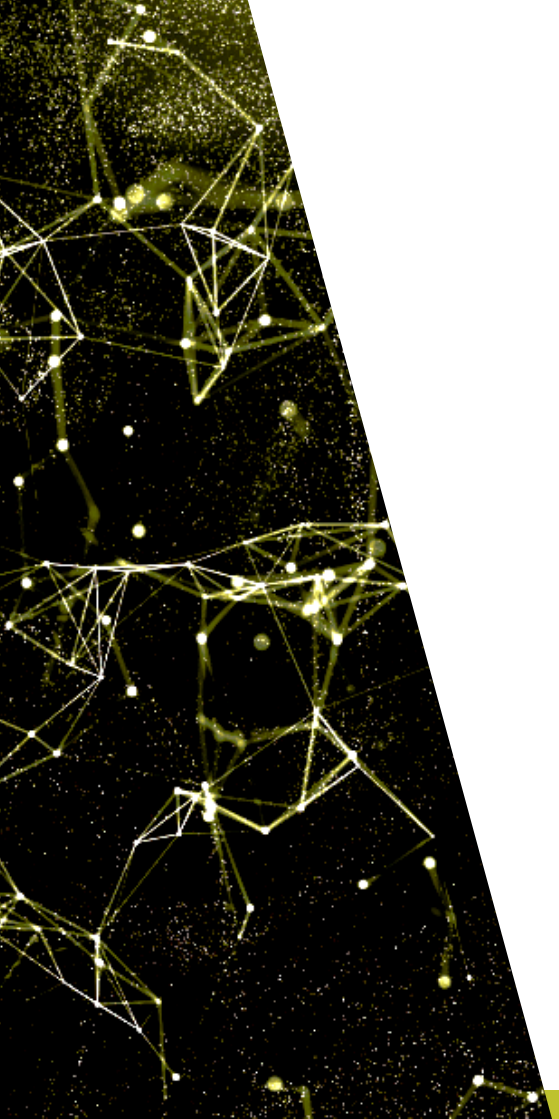
HARRIS KYRIAKIDES

Annual Report on the decisions issued by the Cyprus Commissioner of Personal Data Protection in 2022

Data Protection and GDPR

January 2023



Introduction

This Annual Report summarises the main decisions issued by the Cyprus Commissioner of Personal Data Protection in 2022, in which a penalty was imposed or a warning or recommendation was made due to any form of violation of data protection laws applicable in Cyprus.

Since 25 May 2018, the Cyprus Commissioner of Personal Data Protection has imposed fines in the region of approximately €1.3 million for various infringements of data protection laws.

Previous decisions in relation to fines and penalties under GDPR do not necessarily constitute any binding precedent. GDPR fines are decided on a case-by-case basis and can vary depending upon the circumstances of each case. Therefore, the Office of the Commissioner for Personal Data Protection first and foremost takes into consideration the specific conditions and circumstances of each case when determining fines and penalties when there is an infringement of GDPR.

This report has been prepared by Harris Kyriakides and it does not relate or bind in any way the Commissioner's office.

Complaint for recording personal data without proper legal basis

Facts:

The complainant went to a branch of a courier company, ***(the Complainee***) to pick up a package. Her identification had not been carried out with the tracking number or/and by simply showing her identity document. The Complainee used the Complainant's identification number, which it had recorded in its records. The complainant considered the action of the Complainee excessive and unacceptable, considering that her identification would have been possible simply by showing her iden- tification document. She contacted the Complainee in writing, but the reply she received did not satisfy her; for this reason, she filed a complaint to the Office of the Commissioner for Personal Data Protection (***the Office***).

The Complainee was asked by the Commissioner to specify the legal basis on which the recording of the passport and identity card number of the recipient is based. The Complainee explained the basis on which she considered she could collect the personal data in question. As part of the investigation of the complaint, the Office of the Commissioner of the Electronic Communications and Postal Regulations was contacted, where it was found an absence of a legal basis to justify the processing in question. After this fact was pointed out to the Complainee in the context of issuance of the prima facie decision, the Complainee immediately complied by giving orders to cease this practice and delete any data collected up to that point.

Decision:

Taking into account the mitigating factors, including, inter alia, the fact of the Complainee's prompt compliance at the investigation stage of the case and the lack of intent to infringe GDPR, it was found that, under the circumstances, imposing any administrative penalty or taking any remedial measure was not justified.

For the entire decision press here.

Complaint for receiving spam or unsolicited commercial messages

Facts:

The complainant stated that he receives unsolicited promotional messages from a communications company (***the Complainee***), even though he had terminated his service with the Complainee for that specific number years ago and transferred it to another company. He then added that after each message he received, he called the number to stop receiving messages, but without any result.

The Complainee informed the Office that the complainant is an active customer of theirs with a different phone number, and the number to which the messages were sent was registered as his contact number. During the upgrade of the system that supports the telephone system of the "Stop SMS" service a technical problem arose and, as a result, the orders to stop receiving messages were not properly executed. Additionally, as stated, the technical issue of the "Stop SMS" service was fixed and the number of the complainant was removed from contact number of the service of the other number he had. It has also identified and excluded from SMS promotions all the numbers of the subscribers who called the "Stop SMS" service during the period when the technical problem existed.

Decision:

Based on the above, It was considered that the data of the complainant were collected under a contract/ sale of services and the complainant is a customer of the Complainee as a holder of another number. In any case, there was a breach of Article 106 of Law 112 (I)/2004, as amended, because the Complainee sent unsolicited promotional messages to the complainant, despite the fact that he had repeatedly requested to stop receiving such messages.

An **administrative penalty** of 1500 euros was imposed to the Complainee.

Complaint against the Community Council regarding a possible personal data breach of the complainant or / and lack of cooperation with the Office of the Commissioner

Facts:

A complaint was investigated about a change of postal address, without the complainant's consent, concerning an apartment he has in the community.

Pursuant to paragraph 3 of article 21A of the Immovable Property Law, the Land Registry is required to inform the Council in connection with the transfer of the concerned property in the name of the complainant.

During the first imposition of property tax, the relevant correspondence was sent to the permanent residence of the complainant, which is located in another area. The Council immediately corrected the postal address, following a complaint by the complainant. Therefore, the change in the postal address for the concerned apartment was not due to deliberate or/and malicious action, but to the online update of the Land Registry. Further, according to the evidence the Council has adduced to the Office, it was found that during the purchase of the concerned apartment, the complainant himself declared the address of his permanent residence to the Land Registry.

Decision:

Consequently, it was decided there was no breach of the provisions of the Regulation, regarding the change of postal address and sending the property tax of the concerned apartment, since the change of postal address was due to the annual online update of the Land Registry and further, the property tax of the concerned apartment was sent to the complainant's name in a sealed envelope.

However, in the course of the investigation, a breach of the provisions of Article 31 was found on behalf of the Municipal Council, since the appropriate investigation was not conducted in order to give detailed information to the Office, in the context of exercising its duties as a data controller.

All aggravating and mitigating factors that existed in relation to the incident were assessed and an **administrative penalty** of €2.000 was imposed on the Municipal Council for breach of Article 31 of GDPR.

For the entire decision press here.

Complaint by a public figure for press reports regarding her financial situation

Facts:

The complainant claimed that the the publication of the publishing company (***the Complainee***) about her lacked validity, accuracy, and correctness. During the investigation, two rights were weighted up, the right of freedom of expression and the right to privacy and personal data protection and, after hearing the complainee, a breach of basic principles of GDPR was found, such as legitimacy and accuracy.

Decision:

By Decision dated 4/2/2022, an **administrative penalty** of €10,000 was imposed against the complainee and an Order to remove the publication from the website of all the entities controlled by the complainee was issued.

The Complainee complied with the **Order**, but proceeded to filing an Action to annul the Decision.

Complaint against a Municipality regarding the breach of personal data of the complainant

Facts:

Employee of a Municipality collected, by recording screenshots, and shared to a third unauthorised person documents/photos from the Register of a Municipality that concern the complainant and the authorisation for possession of three dogs.

Taking into account the appropriate measures a Municipality took, before and after the said incident, it was found that the imposition of an administrative penalty was not justified. Given the action of the said employee of a Municipality, **Recommendations** were made to a Municipality to immediately repeat, and at regular intervals, the training of all personnel of the Municipality on the provisions of GDPR.

Decision:

Pursuant to Article 58 (2)(b) of GDPR, Harsh Reprimand was issued to the employee of a Municipality, for breach of Articles 5(1) (a), (b), (f), 6(1) and 29 of GDPR.

For the entire decision press here.

Complaint for the collection of email address upon connecting to the Wi-Fi service

Facts:

A complaint was sent to the Office in which the complainant raised various concerns regarding the processing of personal data by a mall (***the Complainee***). Some of his concerns were answered and/or resolved by the Complainee before the complaint was sent to the Office. What remained to be investigated was the condition laid down to a person who was using the wireless networking (Wifi) service, as to first complete his email address in a corresponding field in order to be provided with that service.

Decision:

In the context of the investigation, it was concluded that the consent which was requested by the data subject in this case had not been given freely. The Complainee also collected more data than it needed both in relation to the purposes for which it relied, and to be able to provide the Wifi service to its visitors, breaching the principle of minimisation (Article 5(1)(c) of the Regulation).

An **Order** was issued to the Complainee to:

(a) Stop collecting the email addresses of data subjects, and

(b) Delete all the email addresses collected for the purposes of providing access to the Wifi.

A specific timeframe was given for compliance. The Complainee informed the Office that, within the timeframe, it has deleted all the email addresses collected and that no personal data of any kind are collected when data subjects are connected to its Wifi. The compliance in any case is being monitored.

For the entire decision press here.

Complaint for breach of personal data

Facts:

The complainant found an article in an online newspaper, which referred to promotions that had been given listing, amongst others, her full name.

After the positions of the company were requested, a breach of Articles 5(1)(a) and 6(1)(f) of GDPR was found, since the nominal publication of promotions is not legislatively provided in such case and furthermore, the company had proceeded to the said publication without weighing up the right of freedom of expression and information and the right of privacy and personal data of the complainant on the other hand, in order to prove that the former prevails.

Decision:

Pursuant to Article 58(2)(d) of GDPR, an **Order** was issued to that company to delete the personal data of the complainant from the said publication within seven (7) days from the day of receiving the said Decision. The Complainee complied with the Order of the Office.

Complaint against doctor for operating a Closed-Circuit Video Surveillance in a common area of two medical centres

Facts:

A complaint against a doctor was submitted (***the Complainee***), with regard to the installation and operation of a Closed-Circuit Video Surveillance, in the common waiting area of medical centres working at the same time.

Through the investigation, it was found that some of the cameras of the CCTV. received footage from the waiting area of the medical centres and from the street and the pavement outside the building. Therefore, I requested from the Complainee to remove the said cameras.

The whole communication of the Complainee with the Office and the delayed response to the matters presented, indicated that the Complainee did not show the appropriate cooperation, as required pursuant to GDPR, with the Office.

Decision:

Taking into account that the Complainee complied with the positions, with delay, a **Reprimand** was issued for the breach of Articles 6(1) and 31 of GDPR, and additionally an **administrative penalty** of €1.500 was imposed for breaching its duty under Article 31 of GDPR.

For the entire decision press here.

Complaint for non-enforcement of the right of access from the Cyprus Police

Facts:

The complainant submitted a complaint through a lawyer to the Office for non-enforcement of the right of access from the Cyprus Police ***(the Complainee***).

It was checked whether the Complainee, after the prima facie decision, as controller, satisfied the request of the complainant for access, according to the provisions of Articles 12 and 15 of GDPR.

According to the information laid down before me, a breach of Article 12 par. 3 of GDPR was found, which concerns the obligation of the controller, in this case the Complainee, to respond to the satisfaction and/or justified rejection of the request of the data subject, within the institutionalised period of time.

Decision:

In view of these information, an **Order** to the Complainee (controller) was issued to establish, within 4 months, namely until 31/7/2022, procedures of submission and enforcement of the rights of the data subjects as the GDPR provides and to communicate them to the Office.

In case the Complainee does not comply with the above **Order** within the abovementioned timeframes, the need to take stricter administrative measures against it will be reviewed with a new decision of the Office.

The compliance with the **Order** is being monitored.

For the entire decision press here.

Complaint for breach of personal data of a hospital worker

Facts:

A hospital worker submitted a complaint to the Office against her employer (***the Complainee***) because another worker emptied the drawers of her office without first having informed her, while the complainant was on sick leave. In the drawers of the complainant there were, inter alia, her medical records and the medical records of her family members.

In the context of investigating the complaint, it was shown that, with her actions the complainant constituted herself a controller, capacity which entails responsibilities according to the provisions of the Regulations. Since keeping original medical records had no legal basis, a Reprimand to the complainant was issued.

Decision:

Taking into account, inter alia, the absence of written procedures of the Complainee regarding moving objects or/and online personal data or/and clearing out drawers, the absence of procedure for the management of the medical records, the failure to detect the absence of the medical records from the Archive of the Complainee, the promotion of internal circulars from the Management of the said hospital, by which it has repeatedly called on the personnel to return to the Archive any medical records it may had in its possession, as well as the fact that the employee who moved the complainant's objects acted arbitrarily, despite the orders of the Management of the Complainee, an **Order** was issued to the Complainee to:

1. Prepare written procedures with regard to the transfer of staff and moving of its personal objects and if it is deemed necessary to updated and/or reinforce the existing written procedures, and
2. Take strict measures in order for the written procedures to be enforced on behalf of the Complainee

The compliance with the **Order** is being monitored.

For the entire decision against the Complainee press here.

For the entire decision against the complainant press here.

Complaint against a judo sports club for the publication of photographic and audio-visual material of a minor on Social Media

Facts:

A father of a minor athlete filed a complaint against the coach of a judo sports club of a rival team. The coach had posted photographic and audio-visual material of the complainant's minor son on Social Media, without having the prior consent from the complainant. The complaint was investigated after the complainant adduced further evidence, according to which the Cyprus Judo Federation had sent a letter to all registered sports clubs on the necessity of obtaining relevant consent from the athletes and/or their guardians before posting photos or audio-visual material on Social Media of any athlete from the sports club in which the son of the complainant practices sport.

Decision:

It was found that the coach of the rival sports club was bound in his professional capacity by the letter that the Cyprus Judo Federation had sent and should have obtained the prior consent of the athlete and/or the guardian of the athlete. Having considered all the mitigating and aggravating factors, the administrative penalty of the **Reprimand** was imposed to the coach for breach of Article 6(1)(a) of GDPR. A **Fine €5000** was further imposed to the Cyprus Judo Federation for non-cooperation with the Office and breach of Article 31 of GDPR, since it never responded to anything that was requested from it during the investigation of the complaint.

For the decision against the coach press here.

For the decision against the Cyprus Judo Federation press here.

Breach of Personal Data in the systems of the Ministry of Defence

Facts:

After being informed through an article posted on the website Secnews.gr that an attack had been carried out on the website "newarmy.mod.gov.cy" of the Ministry of Defence (***MOD)***, the Office carried out an audit at the premises of their processor, regarding the design, development and support of the system that had been attacked.

Based on the exchanged correspondence and the findings of the audit, it was found that with the attack unauthorised access to a MOD system was obtained, which was hosted on the processor.

Following a legal and technical review, a violation of Articles 32 (Processing Security) and 24 (Responsibility of the Controller) was found by the MOD and a violation of Article 32 by the processor.

Decision:

Taking into account all the facts of the case, the technical and organizational measures taken by the two entities prior to the attack and the mitigating factors reported by the companies, an **administrative fine** of five thousand (€5,000) euros was imposed on the MOD for violation of Article 24(1) and 32(1) of GDPR.

An **administrative fine** was imposed on the processor of seven thousand five hundred (€7,500) euros for violating Article 32(1) of GDPR.

The processor filed an appeal against the Decision before the Administrative Court.

Breach of Personal Data

Facts:

After being informed through an article posted on a website that a cyber attack had been carried out on airport's systems, the Office carried out an audit at the premises of the airport and at the processor which acts as the processor, regarding the design, development and support of the system that had been attacked.

Based on the correspondence exchanged, it was found that the attack gained unauthorised access to an Airport system.

After legal and technical review, a violation of Articles 32 (Security of Processing) and 24 (Responsibility of the Controller) of GDPR was found by the manager of the airport and a violation of Article 32 by the processor.

Decision:

Taking into account all the facts, the technical and organisational measures taken by the two companies prior to the attack and the mitigating factors reported by the companies, the following was imposed on the manager of the airport:

1. an **administrative fine** of six thousand (€6,000) euros for violating Article 32,
2. for violating Article 24, the manager of the airport was **Ordered** to:
    a. carry out regular monitoring of the processor's actions; and
    b. revise the contract with the processor to include security measures that need to be taken, which shall be described in an appropriate level of detail in accordance with the nature and environment of the system.

An **administrative fine** of five thousand (€5,000) euros on the processor was imposed.

The processor filed an appeal against the above Decision before the Administrative Court.

Incident of personal data breach of an insurance company's customers at the premises of a processor

Facts:

An insurance company reported to the Office an incident of personal data breach, which occurred at the premises of the processor. The insurance company, as the controller, instructed the processor to print, file and mail three forms, which were the annual premium statements of the customers (beneficiaries and/or insured persons) of the controller.

One form required the insertion of two pages in each policyholder file, which was carried out correctly. The other two forms required the insertion of one page in each policyholder's file. However, the required change in the scheduling of the AutoMailer was not made and therefore two pages per file continued to be enveloped. The omission of the change resulted in half of the recipients receiving, in addition to the form that concerned them, a form of another recipient (and more specifically, the form of the next recipient that was on the list). The controller was informed of the infringement incident by his client, who also received the form of another client. As reported to the Office, the production manager gave clear written instructions to the system operator on the actions to be taken and left his workplace. However, the operator due to "sheer negligence" made a mistake in the programming of the AutoMailer and did not carry out the appropriate sample check, resulting in the incident under investigation.

Decision:

There was a multi-annual cooperation between the controller and the processor, but there was no signed data processing agreement at the material time. Therefore, no processor was used, who provided sufficient assurances for the implementation of appropriate technical and organisational measures, in violation of Article 28(1) of GDPR. In addition, due to the absence of the data processing agreement, it was found that the controller could not prove that the processing was carried out in accordance with GDPR. Therefore, it was found that there is a violation of Article 24(1) and Article 28(1) of GDPR by the controller and imposed an **administrative fine** of three thousand five hundred euros (€3,500).

In the course of the investigation, it emerged that the processor did not implement appropriate technical and organisational measures in order to ensure an appropriate level of security against the risks, as his obligation under Article 32(1) of GDPR, which also derives from his obligation to "take all necessary measures under Article 32", as provided for under Article 28(3)(c) of GDPR. Therefore, having found a violation of the above articles, an **administrative fine** of three thousand seven hundred and fifty euros (€3,750) on the processor was imposed.

Notification of an incident of personal data breach by a Bank

Facts:

Notification of an incident of personal data breach by a bank (***the Bank***) was submitted to the Office, according to which at the end of September – beginning of October 2021, after the sale of the Bank's credit facilities to to a third company, during the process of transferring electronic records of customers and guarantors to the latter, customer data whose credit facilities had not been sold were inadvertently disclosed.

Three instances of accidental disclosures have been reported to the Office. The 1st incident concerned a letter which was sent accidentally by the Bank to to the third company, the 2nd incident involved the inadvertent sending of 11,673 electronic files and the 3rd incident the accidental sending of an electronic file, which included the 45-day letters sent to customers and affected 5,500 data subjects.

Decision:

Upon completion of the investigation, a violation of Articles 5(1)(f), 24(1) and 32 of GDPR were found and an **administrative fine** of €10,000, in relation to the second incident and an **administrative fine** of €7,000, in relation to the third incident were imposed. Finally, a **Recommendation** was given to the Bank, that the Data Protection Officer is informed in advance, before any actions are taken, regarding incidents that may violate the Regulation, and that any decisions on any actions shall be taken jointly.

Complaint about the installation and operation of Closed-Circuit Video-Surveillance in a private company

Facts:

A complaint was filed with the Office regarding the installation and operation of a closed-circuit video-surveillance system (the CCTV) within the offices of a private company (***the Complainee***). During the investigation, it emerged that in addition to the video recording of its interiors, the Complainee was also receiving a picture from public spaces outside its building.

Decision:

Taking into account all the positions of the Complainee and all the data before the Office, a violation of Articles 5 and 6 of GDPR were found and a Reprimand was addressed to the Complainee.

Also, having set out and analysed within the legal framework and the Rationale of the Decision all relevant legal provisions, the **Order was given** as to:

- completely deactivate the CCTV cameras that receive an image inside the offices, waiting areas
- and meetings of its building,
- completely deactivate the external cameras that receive an image from public spaces and places other than its private property, and **Command** as in the event that it takes additional alternative security measures and deems necessary the operation of the CCTV,
- implement appropriate technical and organizational measures, so that the CCTV cameras that may be put into operation are in accordance with the provisions of GDPR.

For the entire decision click here.

Complaint about a leak of personal data of a citizen to a third person

Facts:

A citizen filed a complaint with the Office, against the Electricity Authority of Cyprus (***the Complainee***), regarding a leak of his personal data to a third party. The leak concerned simple category personal data, which was contained in the Complainee's consent form, which instead of being given to the complainant himself, whom it concerned, was given to a third person.

Decision:

As it emerged during the investigation, the Complainee did not ensure, as it should have done, the protection of the complainant's personal data from unauthorised or unlawful processing. Nor had it taken adequate measures in advance to be able to prevent or detect the alleged infringement. Therefore, finding a violation of Articles 5(1)(f), 24(1) and 32 of GDPR, an **administrative fine** of €5,000 on the Complainee was imposed.

For the entire decision press here.

HARRIS KYRIAKIDES

Our Services

We are experts in advising on all aspects of data privacy law and GDPR (General Data Protection Regulation 2016/679), working with our clients on the practical application of data privacy rules, as well as supporting them when they are being challenged under such rules or when they need to comply with data privacy rules. We have serviced many GDPR compliance projects for businesses of various sectors of the economy.

Our key service areas include:

- Reviewing and evaluating your company's data privacy compliance objectives against European privacy laws and regulations including GDPR and helping you to generate and ensure a GDPR compliant work environment in accordance with your business needs and requirements;
- Advising on the use of online advertising and online profiling;
- Representing clients in matters related to violations or investigations pending before the Commissioner for Personal Data Protection and persuing related complaints on behalf of aggrieved clients. In that respect, we also advise on the protection of both personal and sensitive business data against its unauthorised and illegal collection, use, storage, disclosure, transfer and destruction and further use;
- Counseling clients on complex issues associated with legal compliance and business strategy relating to privacy and security risk management, developing internal policies and procedures, and help IT departments in handling cyber security and technology transactions;
- Providing advice on security and transfer of personal data to third countries and provide data processing agreements and other legal tools for such purposes;
- Providing GDPR training, presentations and risk assessments customized to the needs of each company;
- Providing advice on how to handle employees' personal data within multiple countries and jurisdictions;
- Providing legal opinions on specific matters relating to personal data and guidance on how to handle such matters;
- Assisting as external Data Protection Officers (DPO) or as part of your DPO team.

Our Team

Michael Kyriakides
Partner

Michael Kyriakides leads the Commercial & Corporate Litigation & Advisory at Harris Kyriakides.

Expertise
Data Protection and appointment as DPO

Academic Qualifications
MSt, University of Oxford, 2003
LLM, University College London, 2002
LLB, National and Kapodistrian University of Athens, 2001

Professional Qualifications
Member of the Cyprus Bar, 2004
Licensed Insolvency Practitioner

T: +357 24 201600, Ext.: 620
E: m.kyriakides@harriskyriakides.law

Eleni Neoptolemou
Partner

Eleni Neoptolemou is a Partner of the Commercial Team at Harris Kyriakides. Eleni specialises in Data Protection, GDPR audits, representing client before the Office of the Commissioner for Personal Data Protection, and preparation of Privacy Notices, Processing Agreements, Gap analysis and Privacy Policy.

Expertise
Data Protection and appointment as DPO

Academic Qualifications
LLM, University of Central Lancashire - Cyprus, 2017
LLB, National and Kapodistrian University of Athens, 2015

Professional Qualifications
Member of the Cyprus Bar, 2017
Member of the Cyprus Mediators Association , 2022

T: +357 24 201600, Ext.: 754
E: e.neoptolemou@harriskyriakides.law

Munevver Kasif
Associate

Munevver Kasif is an Associate of the Commercial Team at Harris Kyriakides. She specialises in Data Protection, GDPR audits, representing client before the Office of the Commissioner for Personal Data Protection, and preparation of Privacy Notices, Processing Agreements, Gap analysis and Privacy Policy.

Expertise
Data Protection and appointment as assistant DPO

Academic Qualifications
LLM in in Maritime and Transport Law University of Rotterdam, Netherlands, 2014

LLB, University of Dundee, Scotland, 2013

Professional Qualifications
Member of Bar Cyprus Association, 2019

T: +357 24 201600, Ext.: 758
E: m.kasif@harriskyriakides.law

HARRIS KYRIAKIDES

Nicosia
1 Kinyra street, 5th floor
1102 Nicosia, Cyprus

Larnaca
115 Faneromenis Avenue,
Antouanettas Building
6031 Larnaca, Cyprus

Limassol
12 Platonos Street,
3027 Limassol, Cyprus

Paphos
4 Nicou Nicolaidi & Kinyra, 2nd floor,
8011 Paphos, Cyprus

Paralimni
164A Georgiou Gourounia, 1st floor,
5289 Paralimni, Cyprus

Tel: +357 2420 1600 | Fax: +357 2420 1601
Email: info@harriskyriakides.law | Web: www.harriskyriakides.law