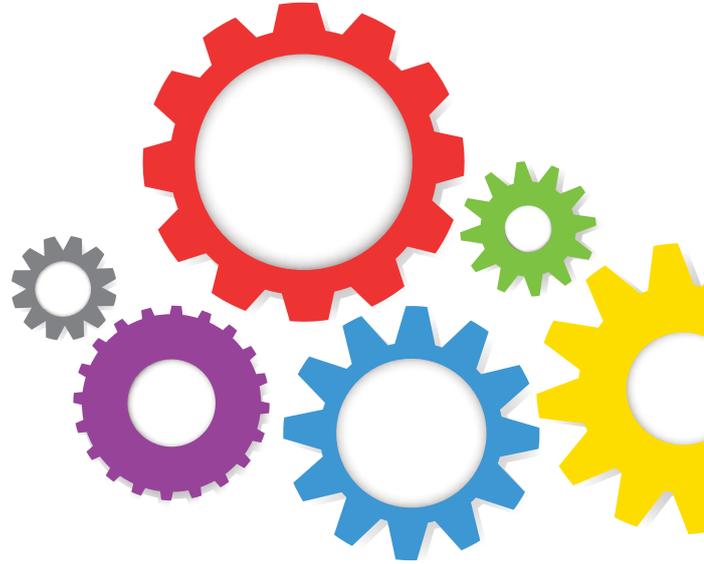




GIBRALTAR REGULATORY
AUTHORITY

Annual Report

2024 / 2025



www.gra.gi

Table of Contents

| | | |
|---|---|-----------|
|  | CHIEF EXECUTIVE OFFICER'S STATEMENT | 5 |
|  | ELECTRONIC COMMUNICATIONS | 9 |
| | Introduction | 10 |
| | International Participation | 10 |
| | Regulatory Matters | 12 |
|  | RADIO COMMUNICATIONS | 19 |
| | Introduction | 20 |
| | International Coordination and Participation..... | 21 |
| | Regulatory Matters | 24 |
|  | INFORMATION RIGHTS | 29 |
| | Introduction | 30 |
| | International Participation | 30 |
| | Local Collaboration..... | 43 |
| | Regulatory Matters | 51 |
|  | BROADCASTING..... | 61 |
| | Introduction | 62 |
| | International Participation | 62 |
|  | POSTAL SERVICES | 67 |
| | Introduction | 68 |
| | Regulatory Matters | 68 |
|  | HIGHER EDUCATION REGULATION..... | 73 |
| | Introduction | 74 |
| | Regulatory Matters | 74 |
|  | CYBER SECURITY COMPLIANCE..... | 77 |
| | Introduction | 78 |
| | International Participation | 78 |
| | Regulatory Matters | 79 |
|  | COMPETITION | 81 |
| | Introduction | 82 |
| | International Participation..... | 82 |
| | Regulatory Matters | 83 |
|  | ACCESSIBILITY | 85 |
| | Introduction | 86 |



CEO Statement



Introduction

This Annual Report of the Gibraltar Regulatory Authority (the “GRA”) is prepared in accordance with section 19(1) of the Gibraltar Regulatory Authority Act 2000 (the “Act”) and covers the period 1st April 2024 to 31st March 2025.

Gibraltar Regulatory Authority Act 2000

The GRA Board currently consists of the GRA’s Chief Executive Officer, Mr John Paul Rodriguez, and two members appointed by the Chief Minister, namely, Mr Charles Bottaro and Mr Francis Carreras.

Organisation and Staffing

The GRA has a total staff of twenty-five and is divided into Divisions, each with their own structure, obligations, and responsibilities. The work carried out by the Divisions is briefly summarised below:

Electronic Communications

The Electronic Communications Division continues to play a pivotal role in regulating Gibraltar’s rapidly evolving communications sector. Its work focuses on ensuring compliance with the Communications Act 2006, promoting competition, and protecting user interests. The Division regularly assesses market conditions, imposing or removing regulatory obligations based on findings of Significant Market Power. Gibtelecom remains the designated Universal

Service Provider following the annual consultation process.

Over the reporting period, the Division enhanced public engagement by significantly expanding its consumer resources and strengthening its presence on social media. It also continues to support media literacy efforts, a growing area of focus under recent legislative amendments. The Division remains committed to transparency, accessibility, and active engagement with consumers to ensure the sector meets the needs of all users in Gibraltar.

Radio Communications

During the reporting year, the GRA restructured its Spectrum and Operations Division to strengthen its radiocommunications function in line with obligations under the Communications Act 2006.

The Division continues to manage all aspects of radio spectrum, including licensing, interference resolution, satellite coordination, and compliance with international regulations. It also oversees Gibraltar’s frequency allocation and supports satellite filings with the International Telecommunication Union, in collaboration with UK authorities.

This year, the Division assumed full responsibility for daily radio licensing duties and remains committed to ensuring spectrum use is safe, efficient, and aligned with both national and international standards.

Information Rights

The GRA, in its capacity as Gibraltar’s Information

Commissioner, remains firmly committed to safeguarding personal data and upholding privacy rights through the robust legal framework of the Data Protection Act 2004 and Gibraltar GDPR. Over the past year, the Information Rights Division has reinforced public trust by actively promoting transparency, enhancing awareness, and ensuring compliance across sectors.

Through a wide range of outreach initiatives—including public campaigns, educational events, and targeted social media content—the Division has strengthened engagement with individuals and organisations alike. Participation in international forums has also ensured Gibraltar’s continued involvement in global data protection dialogue. The Division remains focused on fostering a culture of data protection and continues to provide practical guidance to support both public and private sector compliance.

In addition, the Division continues to oversee the implementation of the Freedom of Information Act 2018 and contributes to international collaboration in this area.

Broadcasting

The Broadcasting Division continues to uphold its regulatory responsibilities under the Broadcasting Act 2012, which include licensing broadcasters, enforcing licence conditions, maintaining broadcasting standards, issuing codes of practice, and promoting media literacy in Gibraltar. The Division works closely with media providers and maintains a strong relationship with the public service broadcaster.

Gibraltar's broadcasting landscape comprises five media service providers, including the Gibraltar Broadcasting Corporation (GBC), which serves as the sole public service broadcaster offering both television and radio services. Other providers include the British Forces Broadcasting Service, Music Box Gibraltar, GFA TV, and Gibfibre VOD. Through effective oversight and guidance, the Division ensures that broadcasting services in Gibraltar remain diverse, compliant, and accessible to the public.

Postal Services

The Postal Services Division continues to regulate Gibraltar's postal sector in line with the Post Office Act 1961 and associated regulations. Its responsibilities include licensing postal operators and ensuring compliance with universal service obligations, with a particular focus on monitoring the Royal Gibraltar Post Office as the designated Universal Service Provider.

Through the setting and enforcement of quality standards, and by issuing targeted guidance, the Division works to ensure that postal services remain efficient, affordable, and responsive to consumer needs. The Division also supports fair competition in a liberalised market while upholding user rights and resolving complaints where necessary.

Higher Education

The Higher Education Regulation Division, established under the University of Gibraltar Act 2015, continues to fulfil its dual

role as the Gibraltar Higher Education Commission and the Gibraltar Authority for Standards in Higher Education. The Division ensures the quality and integrity of higher education by maintaining a register of university qualifications, establishing recognition criteria, and overseeing academic standards through a robust quality assurance framework.

Since the introduction of the Memorandum of Regulation in 2018—and its subsequent update in 2022—the Division has been instrumental in monitoring the University of Gibraltar's compliance with its statutory duties, governance practices, and financial accountability. The GRA remains committed to supporting the University's academic autonomy while promoting high standards in education and training.

Cyber Security Compliance

The GRA continues to oversee Gibraltar's implementation of the EU's Network and Information Systems (NIS) Directive, transposed into local legislation in 2018 to enhance cybersecurity across critical infrastructure sectors. With the NIS 2 Directive coming into force in January 2023, the GRA is actively monitoring its developments and international cybersecurity trends, including regulatory changes in the UK. These efforts ensure Gibraltar remains aligned with evolving global standards and prepared to respond effectively to emerging cyber threats.

Competition

Under the Competition Act

2020, the GRA operates as the Gibraltar Competition and Markets Authority (GCMA), with a mandate to promote fair competition, protect consumers, and support Gibraltar's economic resilience. The GCMA enforces competition rules, reviews mergers, investigates anti-competitive practices, and provides strategic guidance to both HM Government of Gibraltar and industry.

During this reporting year, the GCMA advanced its regulatory framework through the conclusion of key consultations on competition prohibitions and market investigations, while launching new consultations on enforcement procedures. It also strengthened international engagement and knowledge-sharing by participating in global forums and building relationships with peer authorities.

Accessibility Compliance

The Accessibility Compliance Division continues to oversee public sector adherence to the Public Sector Bodies (Websites and Mobile Applications) Accessibility Regulations 2018. Its core mission is to ensure that websites and mobile applications of relevant public bodies are accessible to all members of society, including individuals with disabilities.

Over the past year, the Division has focused on identifying public sector bodies subject to the Regulations, raising awareness of compliance obligations, and working closely with HM Government of Gibraltar and internal teams to improve digital accessibility. The Division has also developed an online complaints mechanism and is preparing further guidance

to support public bodies in enhancing the accessibility of their digital services.

Other Matters

In-house Data Protection Training

As part of its commitment to continuous professional development, the GRA delivered tailored in-house data protection and privacy training to its staff. These specialised modules enhanced employees' understanding of data protection, privacy, and data security, ensuring they are well-equipped to manage personal data responsibly in line with their specific roles and responsibilities.

Revenue and Expenditure

During the 2024/2025 financial year, the total collected was £1,071,408 which was paid into the Consolidated Fund. This compares to expenditure (calculated on a cash basis), for all the GRA's divisions of £2,330,468.



Electronic Communications



Introduction

The Electronic Communications Division (the “Division”) regulates and supervises the electronic communications sector in Gibraltar. The Division ensures that providers of electronic communications networks and/or services (“providers”) comply with any conditions or obligations which have been imposed pursuant to the provisions of the Communications Act 2006 (the “Act”). The Act sets out, among other things, the general functions and objectives of the Division, including the promotion of competition and the interests of users in Gibraltar. The Division is also tasked with fulfilling its statutory objectives in every activity it undertakes as the sector rapidly evolves to ensure that consumer demand for competitive services is met.

The Division continually reviews the electronic communications sector to assess levels of competition and in turn, to determine whether an operator is dominant or not in a particular market. Where a finding of Significant Market Power (“SMP”) is identified, obligations are imposed to alleviate any competition issues. Alternatively, where SMP is not found, obligations are removed through a process of deregulation.

The Division has also continued to designate a provider of universal services annually and although changes have been introduced to the overall process and scope of the consultation, Gibtelecom remains as Universal Service Provider.

The Division has made a concerted effort during the last reporting period to increase its social media activity and significantly revamp its public engagement processes. The Division developed an extensive catalogue of consumer guidance, consumer tools and a long list of FAQs relating to a broad spectrum of useful and relevant subjects. These have been published on the Division’s section on the GRA website; however, significant effort has also been undertaken to make this useful information more accessible to the general public via its various social media outlets. The Division routinely publishes simple to follow, educational and relevant guidance for Gibraltar consumers.

The Division will also be increasing its focus on media literacy, which whilst on-going at present under the GRA’s Broadcasting remit, is likely to see a notable increase in workload as a result of the growing importance of media literacy and amendments to the Act, which impose on the GRA a new duty to

promote media literacy, in particular as to the risk of harm presented by content on electronic media.

The Division remains committed to making itself more accessible to the general public and encourages customers and end-users to actively engage with the team so that it may consider any issues in future. The Division is contactable via its general email address communications@gra.gi.

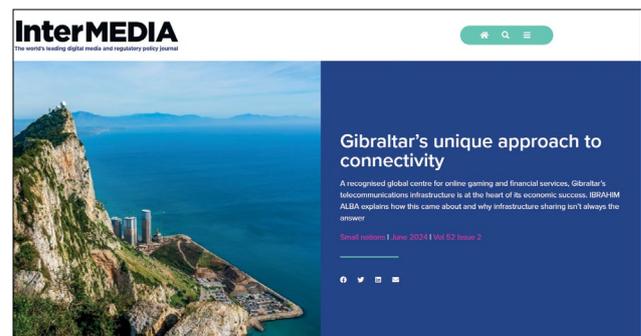
International Participation

International Institute of Communications, Intermedia Journal Article - June 2024 - “Gibraltar’s unique approach to connectivity”

An article written by a member of the Division was published in the International Institute of Communication’s (“IIC”) InterMedia journal.

InterMedia is the IIC’s quarterly journal, renowned for its challenging and often controversial articles contributed by academics, regulators, and industry professionals. It is commonly known as the world’s leading digital media and regulatory policy journal.

The article, entitled “Gibraltar’s Unique Approach to Connectivity” delves into how Gibraltar’s telecommunications infrastructure serves as the backbone of its thriving online gaming and financial services sectors. The article also explores the benefits, regulatory implications as well as the potential limitations of adopting a non-shared approach to telecommunications networks and infrastructure.



International Institute of Communications, International Regulators Forum 4th – 5th November 2024, Bangkok

The Director of Legal and Regulation attended the International Regulators Forum, a key event convening regulatory professionals from across the global communications sector. The forum provided a critical platform for discussion around the most pressing challenges and emerging trends facing regulators today.

Over the course of the event, participants engaged in deep and wide-ranging conversations on topics including:

- The regulatory implications of artificial intelligence, particularly in relation to trust, transparency, and data governance;
- The evolution of mobile networks, with a focus on 5G and future connectivity needs;
- The complexities of regulating digital platforms, including content moderation, market dominance, and algorithmic accountability;
- Challenges associated with low Earth orbit (LEO) satellite systems, such as spectrum coordination, orbital debris, and cross-border licensing.

The second day of the forum

focused on critical consumer-facing issues, including:

- Online safety and protecting users from harmful or illegal content;
- Consumer protection frameworks in the digital age;
- Addressing the growing threat of unsolicited communications, including scams, phishing, and fraud.

The forum was a valuable opportunity to exchange perspectives, gain insight into regulatory approaches from diverse jurisdictions, and reflect on how we, as regulators and stakeholders, can adapt policy tools to keep pace with technological advancement while safeguarding public interest.

International Institute of Communications Small Nations Regulators Forum 5th November, Bangkok

The Director of Legal and Regulation also participated in the Small Nations Regulators Forum (SNRF) — a dedicated space for regulators from smaller jurisdictions to share perspectives, challenges, and policy responses tailored to the unique dynamics of small and developing markets.

At the meeting, the Director of Legal and Regulation was

appointed Vice Chairman of the SNRF. This new role presents an important opportunity to represent Gibraltar's interests on a broader stage. Through this forum, the GRA will be able to bring Gibraltar's specific regulatory concerns into international conversations and contribute to shaping collaborative approaches to common issues among small nations.

This appointment reinforces Gibraltar's voice in global regulatory discussions and supports ongoing efforts to ensure that local policy remains informed, agile, and aligned with international best practices.



International Institute of Communications Annual Conference, 6th- 7th November 2024, Bangkok

Following the International Regulators Forum and the Small Nations Regulators Forum, the event concluded with the International Institute of Communications Annual Conference — a broader gathering that brought together regulators, industry leaders, policy experts, and key stakeholders from across the communications ecosystem. This was also attended by the Director of Legal and Regulation

The Annual Conference served as



a platform for multi-stakeholder engagement and focused on navigating the challenges and opportunities presented by the evolving digital landscape. Key themes included:

- Digital transformation and regulatory adaptation in the age of accelerating technological change;
- Spectrum management, including equitable access, efficiency, and planning for future connectivity needs;
- Strengthening trusted communications, with discussions on privacy, authentication, and the erosion of trust in digital environments;
- Fraud and scam mitigation, with case studies and strategies on preventing misuse of networks and protecting consumers from evolving digital threats.

The conference highlighted the increasing importance of collaborative, cross-sector approaches to ensure that regulatory frameworks remain fit for purpose and capable of addressing both legacy and emerging challenges. It also provided valuable insight into how industry and regulators can work together to promote secure, innovative, and inclusive communications infrastructure and services.



Regulatory Matters

Market Review Universal Service - Public Consultation

On 3rd October 2024, the Division published Public Consultation C03/24 – Designation of Universal Service Provider, seeking feedback from interested parties on various aspects of universal service provision in Gibraltar. The consultation marked an important step in revisiting the approach to the designation of Universal Service Providers (USPs), with the GRA considering the evolving telecommunications landscape in Gibraltar.

Following a comprehensive review of factors such as market shares, network coverage, technology, broadband packages, and service capabilities, the GRA concluded that a revised approach to universal service designation in Gibraltar was needed. The consultation proposed several independent options to address the current state of competition and service provision. One key proposal involved distributing the Universal Service Obligation (“USO”) across all local providers, given that most now offer widespread access across Gibraltar. This would ensure customers’ right to affordable broadband and telephony services. Alternatively, the suggestion to remove Gibtelecom’s USO concerning fixed-location access was driven by the competitive market. This approach would allow market dynamics to guide service offerings, encouraging providers to improve their services and pricing. Removing the USO would also streamline

regulations, reduce unnecessary constraints, and enable a more flexible, market-driven approach that better reflects the current state of broadband accessibility in Gibraltar. However, the GRA remains conscious of the fact that in instances where market dynamics fail, regulatory intervention may not be as swift since no provider is bound by a USO, despite other regulatory powers available to the GRA under the Act.

During the consultation process, the GRA emphasised that consideration should not be limited to market share alone, network coverage is also crucial because it directly impacts the ability of the designated provider to serve all segments of the population. A comprehensive assessment of network coverage ensures that the designated provider can fulfil its obligation to provide universal access effectively. Upon deeper analysis, it became apparent that focusing solely on market shares might overlook providers with extensive infrastructure that can reach more people, thereby potentially compromising the goal of universal service. By prioritising network coverage/reach alongside market shares, the GRA promotes a more inclusive and equitable approach to ensuring universal access to communications services.

By the close of the consultation period, the GRA received detailed submissions from the respondents listed below:

- Gibtelecom
- GibFibre Ltd (“GibFibre”)
- Broadband (Gibraltar) Ltd (“u-mee”)
- Mediatel Ltd (“GibYellow”)

On 12th February 2025, the GRA published Decision Notice C01/25 - Designation of

Universal Service Provider which designated Gibtelecom as USP for the following elements of universal service:

- Provision of access at a fixed location and provision of telephone services.
- Directory enquiry services and directories.
- Public pay telephones and other public voice telephony access points.
- Affordability of tariffs for universal services.

Communications (Amendment) Act 2024

In October 2024, the Gibraltar Parliament enacted the Communications (Amendment) Act 2024, amending the Act. The amendment to the Act essentially prevents the issuing of any new radiocommunications licences in respect of mobile public telephone networks in Gibraltar using technologies such as 2G, 3G, 4G, or IMT/LTE. It is important to note that while no new mobile network providers can enter the market, providers holding such licenses can continue their services and expand their operations within the existing framework.

His Majesty's Government of Gibraltar ("HMGoG") decision to amend the Act and prohibit new mobile network licences from being issued, was the subject of intense debate in the Gibraltar Parliament as some local stakeholders have expressed concerns regarding the potential impact these legislative changes would have on competition and innovation which may create a monopoly that exclusively benefits Gibtelecom. HMGoG said its decision sought to safeguard long-term stability, service quality and consumer

protection within Gibraltar's telecommunications sector.

The impact of the legislative changes on the local telecommunications market remains to be seen. The GRA's public consultation on universal service (as highlighted above) was, to a certain extent, shaped by the knowledge that no new mobile network providers would be entering the market. This led the GRA to having a greater focus on ensuring that existing mobile providers maintain high standards of service and coverage, and that universal service obligations were met in a way that prioritised fairness and accessibility whilst simultaneously addressing possible concerns regarding a lack of innovation, consumer choice and pricing in a market where new entrants are unable to compete with existing mobile providers.

Introduction of "999" Emergency Call Number

The Division is responsible for managing the Gibraltar Numbering Plan and oversees the allocation and assignment of telephone numbers, ensuring they are distributed fairly and in accordance with the rules and procedures set out in the Notice on Numbering Conventions. This includes managing number blocks for various telecommunications services like landline, mobile, and special service numbers (such as emergency numbers).

On 18th March 2024, the new emergency number "999" was introduced as the main number to contact the Royal Gibraltar Police (the "RGP"), Gibraltar Health Authority (the "GHA") and Gibraltar Fire and Rescue Service (the "GFRS"). This single number

has now replaced the number "190" for Fire and Ambulance and "199" or "112" for Police that have been in place for many years. A comprehensive public awareness campaign was conducted by multiple stakeholders to inform the public about the new "999" emergency number, including advertisements, social media updates, and informational materials distributed across the community.

Under the new system, when someone calls "999" they will reach a centralised automated dispatch hotline and hear an automatic reply that will provide them with three options to select from for each of the blue light emergency services, namely:

- Press 1 for Police.
- Press 2 for Ambulance.
- Press 3 for Fire.

The introduction of the new "999" emergency number has standardised Gibraltar's approach to accessing emergency services, making it consistent with both the UK and EU. This change simplifies the process for both residents and visitors, providing an easy-to-remember number to contact emergency services. Additionally, the move is designed to improve the efficiency of emergency call routing and handling, ensuring quicker response times and enhanced coordination between emergency teams.

Currently, there are three local providers, namely Gibtelecom, GibFibre and u-mee, providing fixed/mobile telephony solutions and who are therefore required to provide both residential and business end-users with access to emergency services.

GRA Report - Provision of Access to Emergency Services and Routing of "999" Calls in Gibraltar.

Between July and November 2024, the Division carried out a comprehensive study on the routing of 999 calls in Gibraltar.

The purpose of this study was to assist the GRA, local providers and stakeholders alike in understanding the current state of emergency call routing, mitigation procedures, identify areas for improvement, and ensure that telecommunications infrastructure supports effective emergency response mechanisms. This analysis will provide for a greater understanding of the current emergency call routing mechanisms in place and will also assist the GRA in dealing with any regulatory issues and/or complaints that may arise due to network downtime or a customer's inability to contact emergency services.

To this end, the primary focus was as follows:

- evaluate whether the current routing systems are efficient in connecting emergency calls to the appropriate emergency services (police, fire, ambulance) promptly and accurately.
- determine the reliability of the emergency call routing infrastructure including any back-up or mitigation procedures that may be in place ensuring that calls are not dropped or misdirected, which could potentially lead to delays in emergency response times.
- identify any potential areas where the routing system can be improved, such as optimising call handling procedures, upgrading

technology, or enhancing coordination between telecom providers and emergency services.

- make subsequent recommendations in general (if required) and highlight potential issues that may need to be addressed.

The project remains ongoing and the provision of access to emergency services and routing of "999" calls in Gibraltar will continue to remain under review.

Site Visits - RGP/GFRS/GHA Control Rooms

A crucial element of the Division's "999" report was understanding the internal composition of each emergency service control room when assessing the full end-to-end "999" emergency call service. By knowing the structure and functions of these control rooms, the GRA can better assess how effectively emergency calls are handled. Consequently, two members of the Division carried out various site visits to the various emergency service control rooms after having liaised with the relevant senior officers. These staff members were also granted the opportunity to see first-hand, some of the potential issues being faced with the routing of emergency calls.

Since each control room operates differently, recognising the unique needs/concerns of each emergency service and grasping their internal protocols and capabilities is essential and facilitates performance assessment and enhancement of emergency response systems. Analysing their set-up also reveals opportunities for improvement and innovation, allowing for the implementation of best practices and tailored

solutions where appropriate.

This insight into current operations is not only essential for optimising operations and ensuring public safety in Gibraltar but may also guide future infrastructure development to meet the community's evolving demands.

Gibtelecom - Request for Freefone Numbering Range - (8000-8035)

In response to a request from Childline Gibraltar for an additional free phone number to operate alongside their existing (8008), the GRA took swift action to support this initiative by also contacting Gibtelecom directly and mediating between both parties to ensure a swift allocation. The purpose of the additional line was to be used solely as a dedicated Teen-line and would be used to strengthen their existing services.

As a result, the Division formalised the allocation of a dedicated freephone numbering range (8000-8035) which was allocated to Gibtelecom for "freephone" services. To this end, Gibtelecom are now able to allocate freephone numbers within this range as it sees fit and is not required to seek clearance from the GRA for the allocation of any new services within this range.

Childline Gibraltar had initially requested free phone number (9009), however the Division were unable to allocate this number for numerous reasons, one of which being its similarity to the 999-emergency call number. Ultimately, Childline Gibraltar were granted the additional free phone number (8009) ensuring that they have access to the necessary resources

to offer specialised services for teenagers in need of support.

GRA/RGP - Scam Calls

During the period under review, the Division dealt with numerous queries related to incoming international phone numbers associated with fraudulent activity. This issue has become increasingly prevalent in Gibraltar, as well as globally, with scammers often impersonating legitimate entities, such as bank representatives, to deceive individuals and businesses. The telecoms industry has been particularly impacted, as scammers exploit the anonymity of international calls to target vulnerable individuals. The ease of acquiring phone numbers from foreign networks and the relatively low cost of making such calls contribute to the widespread nature of these scams. As a result, the GRA, the RGP and local telecoms providers, continue to work closely to identify and block these numbers in order protect consumers and businesses from financial harm. Furthermore, the GRA often publishes advice/best practice via its social media platforms to raise as much public awareness as possible.

On 19th August 2024, Gibtelecom received a request from the RGP to block specific international phone numbers linked to fraudulent activities targeting local businesses and individuals. The RGP provided a list of numbers for blocking, which was applied once Gibtelecom received regulatory approval from the GRA. Initially, the block only affected calls routed through Gibtelecom's network. However, these numbers could still enter GibFibre's and u-mee's networks due to the different

routing methods used, such as Session Initiation Protocol ("SIP") trunks. SIP trunks are used to handle and route high-volume voice traffic, including international calls, over fibre-optic connections. These trunks allow voice traffic from other international carriers to reach Gibraltar, which is why calls from these blocked numbers could still bypass Gibtelecom's network when entering other networks. The Division subsequently contacted these operators, who were promptly advised to implement similar blocking measures, leading to the successful resolution of the issue.

A Bill for an Act (The Communications (Amendment) Act 2025) to amend the Communications Act 2006

On 24th March 2025, HMGoG published a Bill for an Act (The Communications (Amendment) Act 2025) to amend the Communications Act 2006. The proposed changes underscores HMGoG's continued efforts to modernise regulatory structures in response to technological advancements, shifting legal landscapes, and evolving societal needs.

This Amendment Act will amend the Act to grant the exclusive privilege to operate a mobile public telephone network to Gibtelecom and to enable the infringement of copyright and other intellectual property rights by network or service providers to be addressed.

Additionally, the Bill includes revisions aligned with the United Kingdom's exit from the European Union, ensuring that communications legislation is fully harmonised with the post-

Brexit domestic legal framework.

At the time of publication, the Act had not been passed at the Gibraltar Parliament.

Local Provider Engagement

The Division has continued to have regular update meetings with local providers, allowing for increased face to face communication, providing a platform to discuss matters at an early stage with the team, potentially preventing issues from escalating, as well as allowing the GRA to offer guidance on any other matters that may arise during these meetings. The Division remains committed to holding regular meetings with providers, as they prove to be an invaluable and constructive endeavour for all involved.

These meetings serve as an essential platform for addressing issues early, enabling proactive discussions that help prevent potential problems from escalating. Additionally, they provide an opportunity for the GRA to offer expert guidance, advice, and clarification on a wide range of matters that may arise. The Division is firmly committed to continuing these regular engagements, recognising their tremendous value in facilitating open dialogue, promoting collaboration, and ensuring that both the GRA and providers can effectively address challenges and seize opportunities for improvement. These meetings have proven to be a highly constructive endeavour, benefiting all parties involved.

Statistical Data

The value of the GRA's Annual Data Gathering Exercise cannot

be understated and remains significant for the Division despite the removal of certain data fields that were no longer considered necessary, during the previous reporting year.

The collection of quarterly statistical data from local providers is a comprehensive exercise that allows the GRA to collect up-to-date and accurate data on the state of the local telecoms sector across a broad range of metrics as follows:

- Fixed & Mobile Telephony
- Broadband Packages
- Residential/Business Subscriber Numbers (including any cancellations/new)
- Ported Numbers
- Call Origination & Call Termination Minutes
- Available International Capacity
- Broadband Traffic

By continuously monitoring these key metrics, the Division ensures that regulatory decisions are informed by real-time insights, enabling it to address emerging challenges, promote healthy competition, and safeguard consumer interests. Furthermore, the data collection process supports the GRA in ensuring compliance with both local and international standards, fostering a transparent and efficient regulatory environment. This ongoing exercise is crucial in terms of both the long-term analyses of the local sector, as well as how it can factor on daily decision making. This is especially true in an ever-evolving sector, where technology and consumer demands are constantly changing. The Division also aims to assess markets almost on a real-time basis by effectively utilising this information as a tool rather than requesting this

as and when needed.

The Division remains committed to working closely with providers to optimise the statistical data requested, as well as continually monitoring and reviewing the guidance available for providers. Recognising that the process of compiling statistics can often be burdensome, the Division regularly reviews and refines the statistics collected as part of the data gathering exercise. In this regard, the Division continues to foster a constructive working relationship with all local providers, who remain dedicated to supplying statistical information in a timely manner. The Division would like to take this opportunity to express its gratitude to these providers.

Statistics and Trends

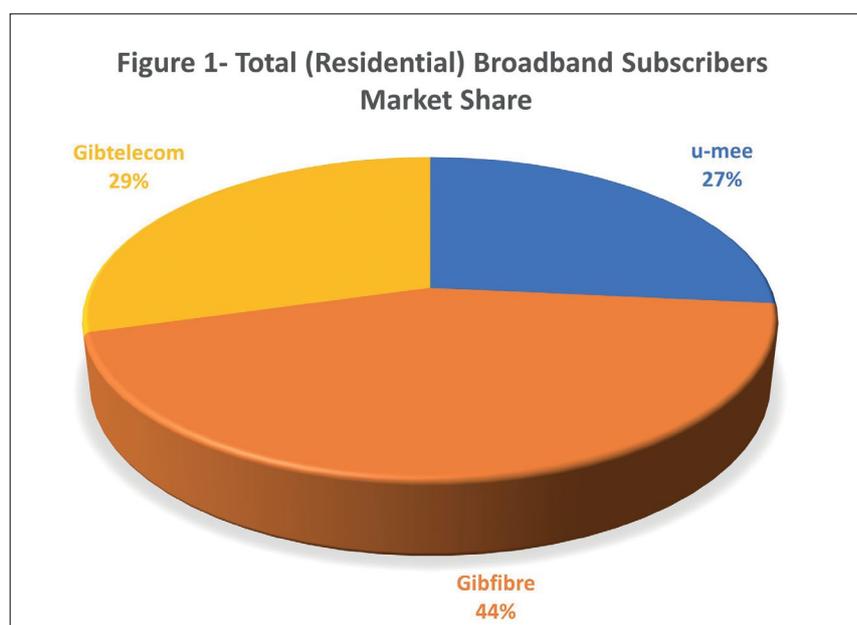
As of March 2025, the total number of broadband subscribers increased from 22,192 in March 2024 to 23,019.

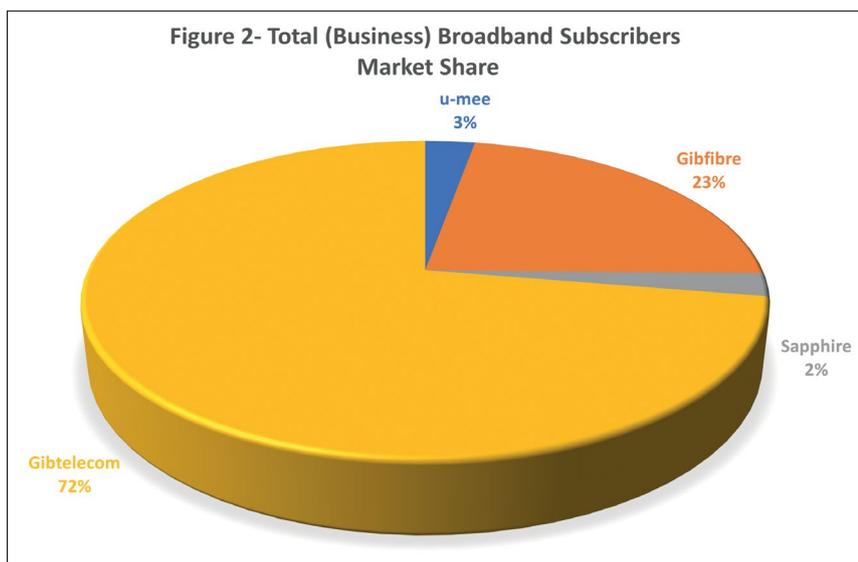
Figure 1 presents an illustration of the fixed residential broadband market shares in Gibraltar as of March 2025. In previous years, this market has experienced the most notable changes, driven

by the increased availability of competitively priced broadband packages and bundles, which led to a significant number of subscribers switching to alternative providers. However, over the past three to four years, the market has stabilised considerably, as anticipated. This likely reflects the trend that consumers are now content with the range of services and packages available, as evidenced by the reduced fluctuations in market shares.

Despite a marginal increase in its residential subscriber numbers during the reporting period, Gibtelecom's fixed residential broadband market share has continued to reduce from 30% in March 2024 to 29% in March 2025.

On the other hand, u-mee's fixed residential broadband market share remain unchanged at 27% as of March 2025. During this reporting period, the local provider that has continued to experience the most significant growth in the fixed residential broadband market is GibFibre, who have increased their market share from 42% in March 2024 to 44% in March 2025, thus cementing their position once





again as the majority shareholder in the local residential broadband market.

Figure 2 shows the fixed business broadband market shares in Gibraltar as of March 2025. In stark contrast to the major shifts in market shares that have been observed in the residential broadband market, the equivalent broadband market for business has experienced considerably fewer changes in market share, both during the period under review as well in the preceding years.

Despite Gibtelecom's market share having decreased slightly from 77% in the previous reporting year to 72% in March 2025, Gibtelecom continues to dominate the fixed business broadband market in Gibraltar. U-mee and Sapphire Network's market shares have effectively remained the same at around 3% and 2% respectively. On the other hand, Gibfibre's market share has again increased from 19% in March 2024 to 23% in the current reporting year. Gibfibre continues to develop its position in both the local broadband markets

It is important to note that many smaller to medium sized businesses purchase residential

broadband products as they often do not require the strict Service Level Agreements (SLA's) and quality of service parameters offered by some business broadband and enterprise solutions. This point should be taken into account when considering these statistics. Unfortunately, this is a variable factor that is beyond the GRA's control, however despite this, Gibtelecom still retains the largest share of the business broadband market.

In addition to this, there are various other reasons why businesses may be less inclined to change provider:

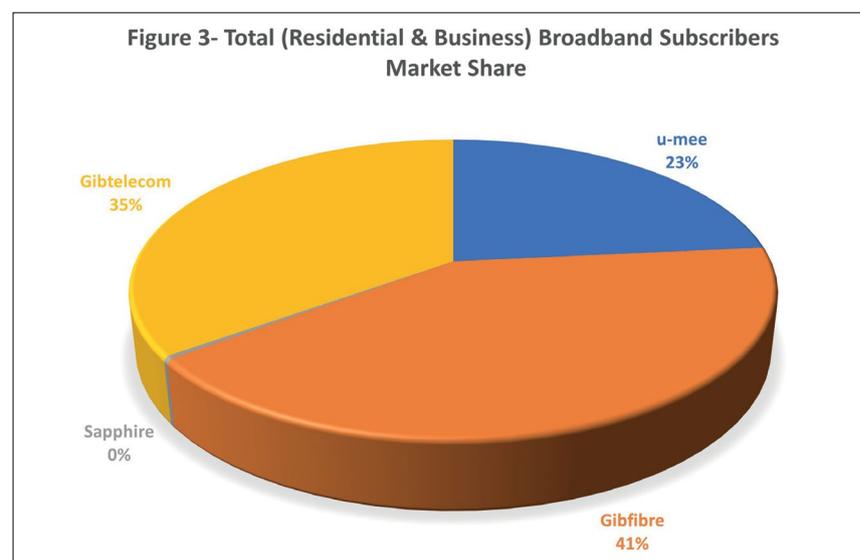
- **Perceived Value:** it appears that some businesses may not

perceive significant differences in the value of the offerings of various business broadband providers, particularly when the services they are currently contracted to meet their needs.

- **Service Reliability and Stability:** Businesses often prioritise reliability and consistent performance over cost. They rely on a stable connection for daily operations, and switching providers could introduce disruptions or uncertainties regarding service quality.
- **Switching Costs:** There can be additional costs associated with changing providers, such as installation fees, downtime during the transition, and the need for new equipment or setup. These costs may deter businesses from frequently switching providers.

Without clear advantages from competitors, there is little incentive for established businesses to change providers despite the likelihood of alternative business packages. These factors combined likely contribute to lower customer turnover in the business broadband sector in Gibraltar.

Figure 3 shows the fixed (residential & business)



broadband market shares in Gibraltar as of March 2025.

Gibtelecom's fixed (residential & business) broadband market share has continued to reduce slightly from 37% in March 2024 to 35% in March 2025. u-mee has also experienced a decrease in its fixed (residential & business) broadband market share, from 24% in March 2024 to 23% in March 2025. During this reporting period, the local provider that has continued to experience the most significant growth in the fixed broadband market is Gibfibre, who have increased their market share from 39% in March 2024 to 41% in March 2025, thus cementing their position once again as the majority shareholder in the local broadband market.

The strength of the residential fixed internet subscriber market in Gibraltar, as touched upon above, represents one of the top destinations in the world in terms of customer choice and broadband speeds. Customers have access to an array of ultra-fast broadband services from up to three service providers, all of whom offer at least some of their services via a FTTH network, with speeds ranging between 20Mbps and 2Gbps.

of the new emergency call number, 999. By sharing timely and valuable information, the Division aims to educate the public, raise awareness, and offer practical guidance on navigating these consumer-related matters. Through its social media channels, the GRA ensures that crucial updates reach the community, empowering consumers to make informed decisions and stay safe in the digital landscape.

Revenue Collected

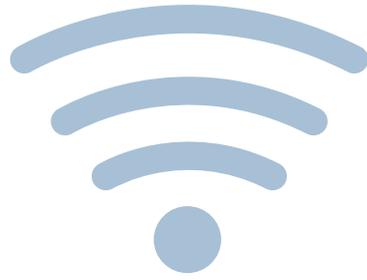
During the 2024/2025 period and in accordance with the provisions of the Act, the total amount collected by the GRA in respect of General Authorisations was £459,057.

The total amount collected by the GRA in respect of Service Providers was £4,050.

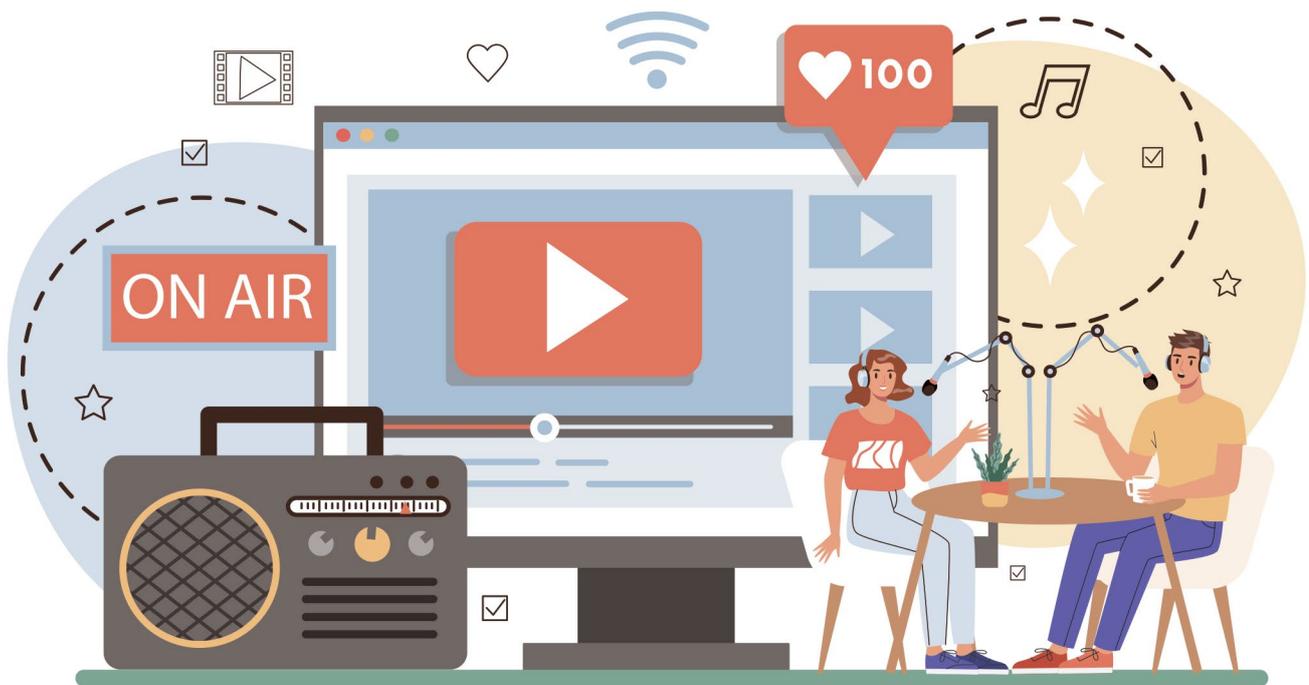
This has brought the total revenue for Service Providers and General Authorisations for the 2024/2025 period to £463,107.

Social Media

The Division actively publishes social media posts to keep consumers and members of the public alike informed on a wide range of relevant topics. These posts often cover important issues such as scam calls, number portability, mobile roaming and the introduction



Radio Communications



Introduction

The GRA's Spectrum and Operations Division (the "Division"), responsible for the management of the electro-magnetic spectrum also oversees internal IT matters and facilities. Radio related matters fell under the jurisdiction of the Director of Legal and Regulation, whilst IT and operational matters were managed by the Director of Information Rights and Operations.

After careful consideration and with a view to further enhance and develop the radiocommunications remit in compliance with the GRA's obligations under the Communications Act 2006, a restructure of the Division was undertaken during this reporting year. An IT Manager was recruited in June 2024 and a team comprising of an IT Manager and IT Officer was established with sole responsibilities for internal IT matters. A Radio Spectrum Officer was later recruited in November 2024 completing the restructure.

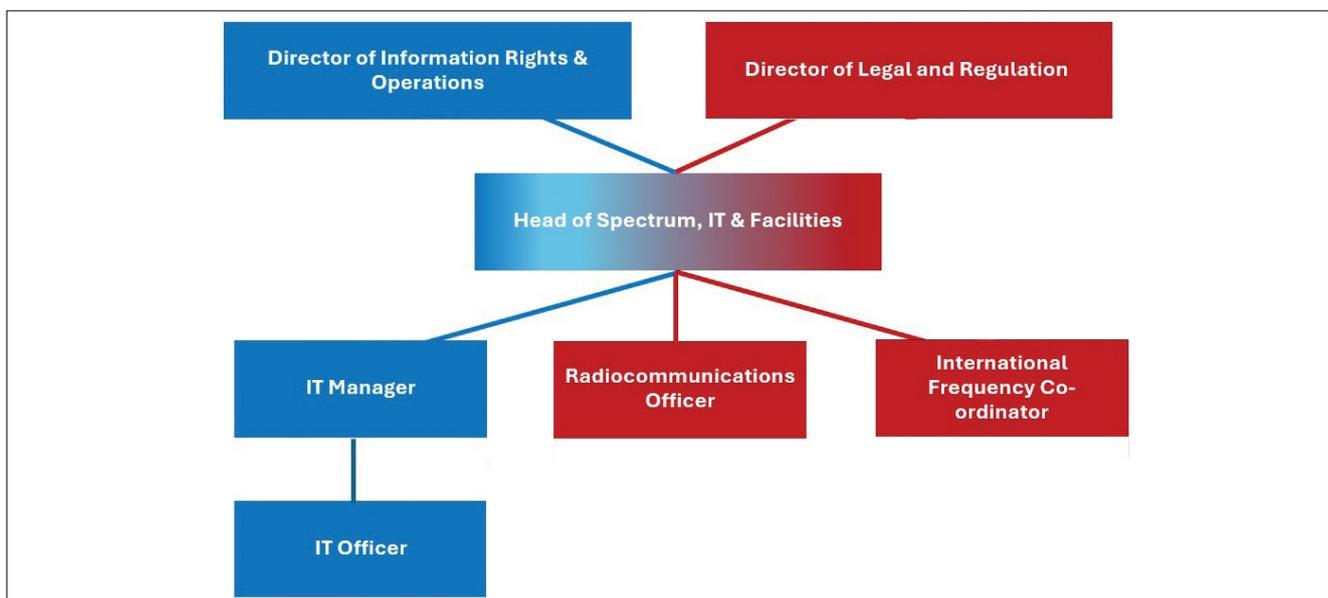
The Head of the Spectrum, IT and Facilities Division retains

overall responsibility for all matters within his remit, though dedicated teams now handle IT and electro-magnetic spectrum related matters separately. Notwithstanding, the International Frequency Coordinator, based in the UK, reports directly to the Head of Division, focusing primarily on attending spectrum related conferences and supporting satellite coordination. The Head of Division is also exclusively responsible for various GRA facilities matters. Furthermore, the Division has taken over all daily licencing duties previously managed by an administration unit, with the exception of payment processing and banking, which remain the responsibility of the GRA's accounts team.

The Division deals with all matters relating to the electro-magnetic spectrum, radiocommunications, radio interference resolution, management of the Gibraltar Frequency Allocation Table, satellite related matters and international coordination. The Division is responsible for administering the regulatory provision of the Radio Regulations, which include

terrestrial and satellite services, together with the issuing of Outer Space Act Licences. The Radio Regulations contain the complete texts as adopted by the World Radiocommunication Conference (Geneva, 1995) (WRC-95) and subsequently revised and adopted by World Radiocommunication Conferences, including all Appendices, Resolutions, Recommendations and ITU-R Recommendations incorporated by reference. Furthermore, the Division also represents the Gibraltar-based operator SES Satellites (Gibraltar) Limited ("SES-G") at international meetings and forums and ensures compliance with the International Telecommunication Union ("ITU") obligations, Radio Regulations and all other international obligations.

The Division examines each new satellite project and carries out the required due diligence before the filing is forwarded to the UK administration for submission to the ITU. The Division assists with the coordination of these satellite networks which are in 8 distinct orbital slots.



As part of its remit under Part VI of the Communications Act 2006 (the "Act"), the GRA is responsible for the management and control of the electromagnetic spectrum. Amongst its duties, the Division carries out regular inspections of sites known to emit radio waves, with a view to ensuring that they operate within the recognised safe guidelines. The Division is also responsible for the management and allocation of radio frequencies, which extend to those used by mobile providers for the provision of mobile voice and data services. The GRA also issues licences to all users of licensable equipment which emit radio waves and has powers to approve radio transmitter equipment to be marketed in Gibraltar.

International Coordination and Participation

Satellite Coordination

The geostationary orbit is where most of the communications satellites are located. At 36,000km above the Earth, the physical nature of the orbit causes the satellite to travel at the same speed as the rotation of the Earth. This means the satellite would be pointing continuously at the same position on the Earth's surface. Conveniently, this means that dish antennas on the ground are kept fixed and pointed at a satellite with no tracking required. This therefore makes

orbital slots and the associated frequency bands used a limited natural resource and the slots must be rationally, efficiently, and economically shared in conformity with the Radio Regulations. The huge benefits of placing a communications satellite in the geostationary orbit has subsequently made it very congested over the years. Any prospective satellites associated with a new filing would need to comply with the regulatory procedures and rules set out by the ITU.

Essentially, all filings can be grouped into two types of services, Fixed Satellite Service ("FSS") and Broadcasting Satellite Service ("BSS"). Once a new filing is submitted to the ITU, the regulatory clock with a 7-to-8-year timeframe for FSS and BSS respectively will commence.

The ITU will examine the filed parameters to calculate the potential for harmful interference these new satellites could cause to existing satellite and terrestrial networks. When the filing is accepted by the ITU, it is published in the bi-weekly International Frequency Information Circulars to inform all other administrations of the new satellite filing.

This starts off the lengthy process of coordination with the operators that are identified as potentially affected, and numerous exchanges of correspondence and meetings are held to complete coordination. Compromises need to be found, and technical parameters adjusted, so that satellites can co-exist and avoid harmful interference.

Once efforts have been made to coordinate the filing, these can be reported to the ITU before the regulatory deadline and entered

into the Master International Frequency Register ("MIFR") which grants it international rights and obligations. When a satellite is placed in the planned orbital slot, it can then bring into use its respective frequency bands.

To date, SES-G has registered 13 filings with the ITU in 8 orbital slots around the geostationary orbit.

Gibraltar has a mature satellite industry and currently has 12 filings brought into use and notified with the ITU, with the activity this reporting year going into existing key orbital slots. These SES-G existing networks could potentially suffer harmful interference from new incoming filings and the Division has identified 99 satellite networks from different administrations around the world that could potentially affect SES-G networks (this includes potential harmful interference identified from the same network under different provisions under the various articles/appendices of the Radio Regulations) or terrestrial services in Gibraltar.

Coordination Requests sent to Administrations

When administrations from other countries submit new filings close to the Gibraltar orbital slots, they have the potential to cause harmful interference. The Division must examine the publications of these new networks and inform the relevant administration that coordination is required. The GRA's in-house developed software drastically reduces the 'analysis time' and therefore allows for more time to consult with the satellite operator before the expiry of the period for comments/objections. This software

application also automates the process of notification to and from Ofcom, the UK regulator, and streamlines the back office associated activities.

Satellite Coordination Meetings

The Division was invited to participate in one administration level bilateral satellite coordination meeting during the period of this report. The planned meeting was with China. However, after liaising with SES-G, it was concluded that the current status of satellite coordination with operators from the respective administrations was satisfactory and it was therefore decided that the Division and its operator would not need to participate in this meeting.

SES-G Development Plan Review Meeting

A meeting was held between the Division, Ofcom and SES-G in June 2024 to discuss the Annual Development Plan update for the SES-G satellite filings. The updated plan was reviewed and approved by the Division prior to discussions with Ofcom. The review with Ofcom was successful, where all points of the Plan were addressed.

Terrestrial Coordination

As with satellite coordination, the Division examines the information published by the ITU with respect to terrestrial services which contains additions, modifications or suppressions of terrestrial transmitting stations or networks from neighbouring countries, any of which could cause interference to Gibraltar

registered stations. Unlike satellites which can cause interference issues to many other satellites or administrations, terrestrial services can mainly affect neighbouring countries, in Gibraltar's case, Spain and Morocco. Notwithstanding their relative distance from Gibraltar, modifications from Algeria and, to a much lesser extent, Portugal, are also examined. Over the period 2024-2025, a total of 71098 modifications including suppressions have been submitted to the ITU, of which 2581 have been examined and only a handful of objections have been raised due to the high probability of potential interference.

ITU World Radiocommunication Seminar 2024 (WRS-24)

The GRA attended the WRS-24 seminar which took place in Geneva from the 2nd to 6th December 2024. The ITU organises World Radiocommunication Seminars ("WRS") on a biennial basis, in conjunction with the cycle of Regional Radiocommunication Seminars. WRS deal with the use of the radio-frequency spectrum and the satellite orbits, in addition to Radio Regulations.

The seminar is primarily split into two main components, the plenary sessions and the terrestrial and space workshops

which run in parallel. The seminar provides hands on experience and updates on the changes to the Radio Regulations including changes to and advances in software applications and amendments to procedures implemented as a direct result of the outcomes of the World Radio Conference which concluded in December 2023.

The seminar also provides a valuable opportunity to meet up with fellow regulators. During the WRS-24, the GRA also attended a Commonwealth ITU Group meeting which was chaired by Ofcom. Attendants from various Commonwealth countries such as India and Canada also took part.

Counter-Uncrewed Aerial Systems ("C-UAS") Workshop

At the invitation of the Director of Civil Contingencies and Civil Aviation, the Division's Head of Spectrum was invited to attend the C-UAS workshop which took place in Gibraltar in March 2025. The workshop also provided an opportunity for the GRA to contribute to the discussions from an electro-magnetic spectrum management perspective and provide insight on how certain counter measures could be implemented without adversely affecting other systems.



Preparations for the next ITU-R World Radiocommunication Conference 2027 (WRC-27)

Whilst the next World Radiocommunications Conference, under the auspices of the ITU, is not until November/December 2027 (WRC-27), the study activities necessary to address all the technical and regulatory issues due to be considered at the Conference are now ramping up and will further intensify over the next few years.

The study activities are undertaken at national (UK), regional (Europe via the European Conference of Posts and Telecommunications ("CEPT") and global level (ITU-R). The Division participates in several of the UK preparatory groups such as IFPG WG3 which is responsible for most of the satellite agenda issues and IFPG WG1 which provides the forum for UK deliberations on International Mobile Telecommunications (IMT) agenda issues. The UK preparatory groups develop the UK positions and brief for each agenda item and agree UK contributions to the CEPT groups and/or ITU-R. The Division participated in approximately ten UK preparatory meetings during this reporting period.

The Division also participates in several European groups, e.g. Conference Preparatory Group Project Team B (CPG – PTB) – the preparatory group dealing with the majority of the satellite issues to be considered at WRC-27 and also in the Conference Preparatory Group ("CPG2") which is the senior group that coordinates and manages all the sub-group activities and approves the final CEPT Briefs and associated European Common Positions ("ECPs") for the various conference agenda

Items. The Division participated in two meetings of the CPG and two meetings of the CPG PTB during this reporting period.

The final agreed texts that emerge from all this study activity will be distilled into the Conference Preparatory Meeting Report which is a key input contribution to the WRC-27 Conference. This Report provides a very useful compendium of the technical and regulatory material that has been considered, discussed and where possible agreed by relevant experts. The Report also includes possible options that address the issues specified in the relevant agenda items.

Some of the key issues under study for WRC-27:

International Mobile Telecommunications ("IMT")

The conference will consider the identification of additional frequency bands for IMT based on the outcome of studies into sharing and compatibility if IMT (5G/6G networks) were permitted in three specific frequency bands between 4.4 – 15.35 GHz.

Mobile Satellite Service ("MSS") in IMT bands

There is considerable interest to consider studies on possible new allocations to the mobile-satellite service for direct connectivity between space stations and IMT user equipment to complement terrestrial IMT network coverage, i.e. to facilitate Direct-to-Device (D2D) communications. The studies are considering technical, operational and regulatory matters of such an allocation to the MSS in bands that are used by the IMT networks (4G/5G) between the frequency range

694/698 MHz and 2.7 GHz.

Earth Stations in Motion ("eSIMs")

There is an agenda item for WRC-27 that requires studies to be conducted into the technical and operational conditions for the use of eSIMs in the 40/50 GHz bands for aeronautical and maritime eSIMs operating to geostationary and non-geostationary space stations. This follows on from work that was concluded at the previous conference regarding eSIMs operating in lower frequency bands.

Access to higher frequency bands for Non-Geostationary Satellite Orbit and Geostationary Satellite Orbit use by the Fixed Satellite Service

The opening up of higher frequency bands for satellite services has been a talking point over recent conferences and WRC-27 will continue that theme by considering technical and regulatory measures for the Fixed Satellite Service for equitable access to the frequency bands 37.5-42.5 GHz (space-to-Earth), 42.5-43.5 GHz (Earth-to-space), 47.2-50.2 GHz (Earth-to-space) and 50.4-51.4 GHz (Earth-to-space).

UK Spectrum Policy Forum – ("SPF")

The Division participates in the quarterly Plenary meetings of the SPF and also in a number of the sub-groups that support the work of the SPF such as Cluster 1 which considers future demand for electro-magnetic spectrum, Cluster 2 which considers

techniques for the sharing of electro-magnetic spectrum, and Cluster 4 which considers WRC activities. The SPF is a forum of UK stakeholders that develop positions on current and future electro-magnetic spectrum policy and provide a sounding board to the UK government.

Regulatory Matters

Below is an overview of regulatory matters dealt by the Division during 2024/2025:

Management of the Electro-Magnetic Spectrum

Section 56 of the Act provides that the ownership of the electro-magnetic spectrum in Gibraltar shall “vest exclusively in the Government and the Minister shall be responsible for its management and control”, and that the Minister “may appoint, in writing, any person appearing to him to be suitable to exercise any of his powers, tasks, duties or functions in relation to the management of the electro-magnetic spectrum in Gibraltar.”

The above-mentioned responsibility has been assigned to the GRA and, as part of its annual remit, the Division carries out regular inspections of the electro-magnetic spectrum using equipment capable of measuring interference, the power levels of equipment transmitting radio waves, and several other factors useful in determining the state of Gibraltar’s electro-magnetic

spectrum usage.

The Division also carries out compliance monitoring to ensure emissions from transmitters comply with international guidelines as set by the International Commission on Non-Ionizing Radiation Protection (“ICNIRP”). As part of the licensing process, the Division conducts annual site inspections on all mobile base station installations and routinely audits base stations throughout Gibraltar for compliance. Full details of these inspections can be found on the GRA’s website. All site inspections, electro-magnetic spectrum audits, and interference investigations, are conducted by trained staff using industry-leading analysers that can identify the power, frequency, and general direction of most transmitters within the 9 kHz – 22 GHz range.

Due to the high volume of buildings and Gibraltar’s topography, locating the source of interference can be challenging. The GRA is not responsible for establishing the recommendations for exposure to electro-magnetic emissions. Therefore, the Division does not set emission safety levels and it has neither the expertise nor the remit to participate in matters concerning biological or health research. The Division has, however, been working closely with the Ministry for the Environment to ensure that concerns from the public regarding electromagnetic emissions from mobile base stations and other radio transmitters are addressed swiftly.

Interference and Power-Level Monitoring

The Division also carries out inspections if concerns are raised by members of the public and/or organisations alike, where there is a suspected case of interference with, or misuse of, Gibraltar’s electro-magnetic spectrum, such as transmission at power levels beyond those recommended by the Division or exceed the ICNIRP Guidelines, the standard adopted by HM Government of Gibraltar. Taking into consideration the resources required to ensure all radio transmitters, including future mobile network base stations, are compliant with the ICNIRP guidelines, the GRA continuously monitors electromagnetic fields (“EMF”) levels throughout Gibraltar and emissions from mobile phone base stations, including all radio transmissions in the frequency band 20MHz to 40GHz.

The monitoring equipment consists of four fixed monitoring units (“FMU”), an indoor deployable unit (“IDU”) (for use inside buildings) and a handheld portable unit (“HPU”) to measure EMF levels at key locations around Gibraltar. The fixed and deployable units monitor the EMF levels in real time in the bands 20MHz to 40GHz and automatically uploads the information onto a publicly available portal. This portal can be accessed via the GRA’s website. This equipment complements the existing analysers which are used primarily to identify the sources of interference and conduct detailed compliance verification.

The table opposite shows the peak and average levels recorded during the measurement programme which launched in April 2021 for this period (1st

April 2023 to 31st March 2024). The results demonstrate that the recorded levels did not exceed the ICNIRP guidelines and on average are well below the maximum threshold.

University of Gibraltar

Peak: Offline- V/m

Average: Offline V/m

Westside/Bayside School Complex

Peak: 6.61.46 V/m

Average: 1.55 V/m

St Anne’s School

Peak: 6.37 V/m

Average: 3.39 V/m

Kings Way House Alameda

Peak: 12.12 V/m

Average: 1.8 V/m

Supplementary to the FMU measurements, the GRA has undertaken an ‘EMF Spot Check’ project targeting locations in near vicinity of mobile base stations, radar, broadcasting stations or areas of public interest such as schools. These weekly spot checks are carried out across six general districts around Gibraltar as shown below, with the primary aim of conducting at least a spot check in all the six districts once a week:

- North District
- South District
- East Side
- West Side
- Beaches
- Schools (excl. summer holidays)

The table opposite shows the peak and average EMF levels recorded between November 2024, and February 2025. The results confirm that all recorded levels remain within ICNIRP guidelines and are, on average, well below the maximum threshold.

| Date Carried Out | Location | Average Measurement |
|------------------|---|---------------------|
| 7.11.24 | GRA | 3.311 |
| 8.11.24 | University Car Park | 3.64 |
| 8.11.24 | Catalan Bay Bus Stop | 3.81 |
| 8.11.24 | Kingsway | 7.05 |
| 8.11.24 | Small Boats Marina | 3.83 |
| 13.11.24 | Sundial - North Corner by Old Cepsa | 8.51 |
| 13.11.24 | Waterport Road - Entrance to Mons Calpe Mews | 5.29 |
| 13.11.24 | Outside St Joseph’s School | 5.49 |
| 13.11.24 | Outside St Bernard’s School | 4.67 |
| 15.11.24 | Eastern Beach Road | 6.15 |
| 15.11.24 | Gibraltar Airport | 6.68 |
| 19.11.24 | Grand Battery House | 5.79 |
| 19.11.24 | Orange Bastion | 2.95 |
| 19.11.24 | Rooftop Boyds - Kings Bastion | 4.08 |
| 19.11.24 | Europa Pool Car Park | 2.13 |
| 19.11.24 | Western Beach Car Park | 4.32 |
| 21.11.24 | Kingsway Foot Bridge | 8.07 |
| 21.11.24 | Top of Eastern Beach Car Park | 8.27 |
| 21.11.24 | Catalan Bay Bus Stop | 5.04 |
| 21.11.24 | Europa Point Cafeteria | 5.41 |
| 27.11.24 | Small Boats Marina | 4.45 |
| 27.11.24 | Morrisons Car Park | 3.18 |
| 27.11.24 | Casemates Square | 5.76 |
| 27.11.24 | John Mackintosh Square | 5.26 |
| 29.11.24 | West View Park | 6.41 |
| 29.11.24 | Ragged Staff Gates | 5.56 |
| 29.11.24 | New Harbours Deck | 7.68 |
| 03.12.24 | University Car Park | 2.48 |
| 03.12.24 | Lathbury Sports Centre Car Park | 1.83 |
| 03.12.24 | Princess Caroline’s Battery | 2.88 |
| 03.12.24 | St Mary’s School Car Park - Town Range | 2.84 |
| 05.12.24 | Sundial - North Corner by Old Cepsa | 6.584 |
| 05.12.24 | Waterport Road - Entrance to Mons Calpe Mews | 2.832 |
| 05.12.24 | Europort Avenue - Outside St Bishop Fitzgerald School | 2.937 |
| 05.12.24 | Outside St Bernard’s School | 2.012 |
| 07.01.25 | Catalan Bay Bus Stop | 6.78 |
| 07.01.25 | Kingsway Foot Bridge | 7.79 |
| 07.01.25 | Gibraltar Airport | 6.67 |
| 07.01.25 | Western Beach Car Park | 4.45 |
| 10.01.25 | Europa Pool Car Park | 6.42 |
| 10.01.25 | Grand Battery House | 4.6 |
| 10.01.25 | West View Park | 4.71 |
| 21.01.25 | University Car Park | 7.16 |
| 21.01.25 | Lathbury Sports Centre Car Park | 7.13 |
| 21.01.25 | Princess Caroline’s Battery | 7.87 |
| 21.01.25 | St Mary’s School Car Park - Town Range | 6.89 |
| 04.02.25 | Kingsway Foot Bridge | 10.85 |
| 04.02.25 | Top of Eastern Beach Car Park | 8.07 |
| 04.02.25 | Both Worlds Bus Stop | 2.74 |
| 04.02.25 | Sundial - North Corner by Old Cepsa | 7.48 |
| 04.02.25 | Small Boats Marina | 4.01 |

Calibration and Maintenance

The monitoring equipment undergoes regular maintenance, and when necessary, is shipped to the relevant manufacturer for calibration. To ensure operational continuity, the calibration cycle for the FMUs has been carefully planned. The site at the Gibraltar University has been temporarily taken offline to maintain three active FMUs operational while one unit is sent for calibration. Once the calibrated unit returns, it is deployed to an active site, and another unit is sent off for calibration in its place. As for the HPU, it was sent for calibration in late February 2025 and is expected to return by the end of May 2025. Upon its return, the Division will promptly resume weekly inspections.

In the period 2024/2025, the following matters were attended to:

a) Air Traffic Control (ATC) Interference

Although interference reports affecting the radio communications between ATC and commercial airplanes have declined, they are all investigated with urgency. In extreme cases, flights could be potentially diverted or cancelled for safety reasons if clear communications with the aircraft cannot be established. Unfortunately, other reports of elevated noise levels, sporadic speech or even music breaking through are harder to pinpoint if they are short lived.

b) Mobile Telephony Interference

In collaboration with local mobile telephony providers and stakeholders, an ongoing interference issue affecting the 700 MHz band used for the provision of 5G services in Gibraltar and as reported by the GRA in 2023/2024, was

located and the interference removed. Notwithstanding, various reports of different varying interferences have been reported over the period and investigated. Due to the nature of intermittent interference with no fixed pattern or regularity, the GRA continues to work closely with providers and users of electro-magnetic spectrum to identify and remove sources of interference.

Advice and Cooperation with other Agencies and Associations

The Division continues to work closely with the Ministry for the Environment and HM Government of Gibraltar agencies to address issues relating to radiocommunications, especially perceived health risks from radio transmitters on existing or new installations. The GRA also meets regularly with other stake holders and operators including the Ministry of Defence to promote the effective use of radiocommunications in keeping with our international obligations and the Radio Regulations.

Licensing of the Electro-Magnetic Spectrum

The GRA collects licence fees on behalf of HM Government of Gibraltar and uses different licensing schemes to promote the use of technologies and maximise the use of the electro-magnetic spectrum efficiently. The following table outlines the fees collected during the period 2024/2025 for each type of licence issued under Part VI of the Act:

| | |
|------------------------|----------|
| Accounting Authorities | £6,522 |
| AGRS | £465 |
| CB Radio | £60 |
| Fixed Links | £5,357 |
| Mobile | £492,261 |
| Radio Microphone | £156 |
| Paging | £0.00 |
| PMR | £8,241 |
| Port Ops | £3,231 |
| Radar | £331 |
| Radio Amateur | £360 |
| Ship Station Licence | £26,725 |
| Wireless Dealers | £1,454 |
| Spectrum Usage | £10,923 |
| VSAT | £2,206 |

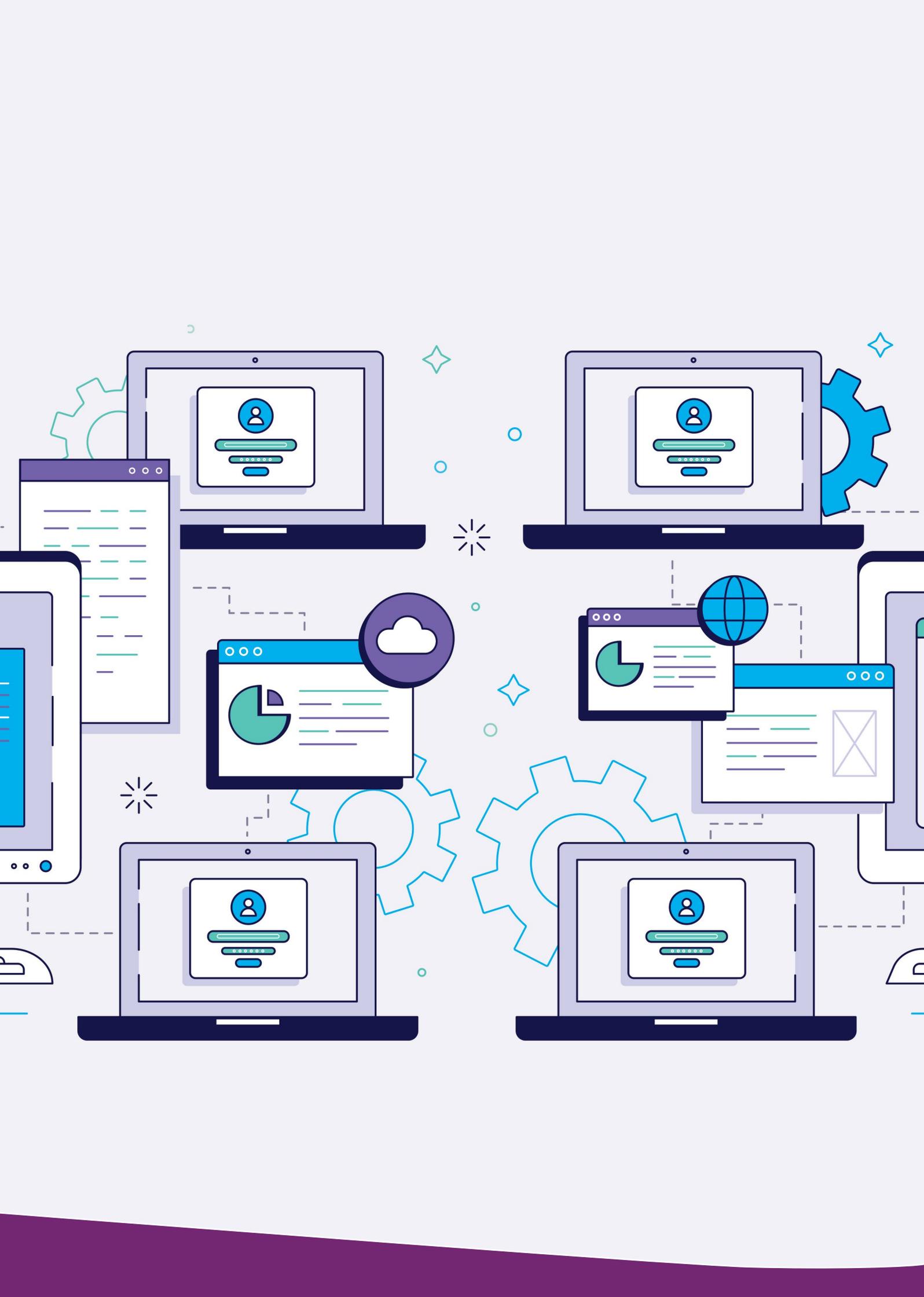
Furthermore, during the period 2024/2025, the GRA renewed five Outer Space Act licences for SES-G for each of the satellites operating in outer space, and which are controlled from Gibraltar. The total revenue received as a result of issuing these licences was £5,000.

Outer Space Act

The UK's Outer Space Act 1986 was extended to Gibraltar by the Outer Space Act 1986 (Gibraltar) Order 1996, which conferred licensing and other powers to the Governor of Gibraltar to ensure compliance with the international obligations concerning the operation of space objects and activities in outer space by individuals associated with Gibraltar. These powers, duties, and responsibilities were delegated to the GRA, by the Delegation of Functions (Outer Space Act 1986 (Gibraltar) Order 1996) Notice 2001.

All the satellites licensed by the GRA are included in the UK's Registry of Space Objects and the Division works closely with the UK Space Agency ("UKSA"), to ensure that the satellites

are operated in compliance with international treaties and principles covering the use of outer space. Since July 2021, the Civil Aviation Authority has served as the UK space regulator, assuming the responsibilities and powers previously held by the UKSA for this role.



Information Rights



Introduction

Gibraltar's data protection framework is underpinned by the Data Protection Act 2004 (the "Act") and the Gibraltar General Data Protection Regulation (the "Gibraltar GDPR"), together forming a robust and modern legislative regime that safeguards individuals' personal data and privacy rights. As the designated supervisory authority, the GRA, in its role as Information Commissioner (the "Information Commissioner"), is responsible for ensuring compliance with these data protection laws.

Over the past year, the Information Rights Division (the "Division") has been instrumental in upholding data protection standards, enhancing transparency, and reinforcing public trust in the GRA's commitment to information rights. Recognising the ongoing importance of collaboration with regulatory counterparts and industry stakeholders, the Division has actively engaged in international and local events, strengthening Gibraltar's position in global data protection discussions.

Key initiatives have included heightening privacy awareness campaigns, including a public Data Protection Survey and a Day in Town event, to educate individuals and organisations on their data protection rights and responsibilities in an evolving digital landscape. Additionally, increased participation in international forums has allowed the GRA to contribute to global data protection efforts and foster cross-border cooperation. Through these initiatives, the Division aims to continue promoting information rights whilst navigating the challenges

of an increasingly interconnected world.

As in previous years, the Division remains committed to providing guidance on data protection matters to individuals, as well as to the private and public sectors. Utilising a multi-channel approach to awareness and education, the Division publishes guidance notes, communicates via email and telecalls, disseminates informative social media content—including audio visual material—and publishes quarterly e-newsletters. Additionally, in-person engagements, such as school visits, further supports the Division's outreach efforts. This year, targeted social media campaigns have focused on several topics, including the requirements of a Data Protection Officer ("DPO"), key findings of the Privacy Awareness School Survey and "A Privacy-Proof Countdown to Christmas" which proved to be engaging. These campaigns have helped reinforce public understanding of data protection and privacy matters.

Separately, the Division continues to oversee the regulation of the Freedom of Information Act 2018 ("FOIA") and will, as appropriate, engage in international workshops alongside other freedom of information regulatory authorities.

International Participation

In fulfilling its responsibilities under the Act and the Gibraltar

GDPR, the Information Commissioner works closely with international Data Protection Authorities ("DPAs") and other key stakeholders. This collaboration encompasses mutual assistance and cooperation in cross-border investigations, as well as the development of best practices and standards for the regulation and enforcement of data protection laws.

The Information Commissioner's ongoing commitment to being a respected and recognised authority within international data protection circles, along with staying informed on the latest developments in the regulatory landscape, has led to Division members taking part in various international events throughout the reporting period.

13-16 May 2024 – European Conference of Data Protection Authorities ("ECDPA")

The ECDPA, known as the 'Spring Conference', is an annual event, which the Division participates as an accredited member. It serves as a platform for European DPAs to collaborate, share perspectives and best practices on privacy and data protection issues.

This year, the Spring Conference was hosted by the Latvian DPA. The event featured two full-day closed-session discussions (for members only) and an open session where DPOs could participate, either online or in person. The sessions covered a range of topics, including:

Tech revolution. With innovation cycles getting shorter, technology is advancing at an unprecedented pace, very often driven by data. These developments underscore the need for DPAs to evolve,

be creative and adopt a forward-thinking approach in keeping with technological developments. The importance of stakeholder engagement was highlighted, along with the growing recognition that effective regulation increasingly involves technologists and other relevant professionals other than legal expertise, to strike the right balance.

Court of Justice of the European Union (“CJEU”) and European Court of Human Rights (ECHR).

Recent decisions from the CJEU and the ECHR were discussed. For example, Case-162/22 where the CJEU ruled that retained data provided to authorities for the purposes of combating serious crime cannot be used in the context of investigations for a disciplinary offence. In the context of the ECHR, a couple of the cases highlighted were – 1) In *Russia v Podchasov* no. 33696/19 the court held that laws requiring the decryption of encrypted messages violated Article 8 of the European Convention on Human Rights (“Convention”) and, 2) In *Drelon v. France* no. 3153/16, the court held that the collection of data relating to a potential blood donor’s presumed sexual orientation (including excessive retention period) violated Article 8 of the Convention.

The evolving and expanding role of DPAs. The discussion highlighted the increasingly important and dynamic role of DPAs, particularly as data protection law continues to intersect with a range of other developing areas, such as - the prevention of illegal/harmful activities (e.g. EU Digital Services Act), data sharing and reuse (e.g. EU Data Governance Act), ensuring fair and open digital markets (e.g. EU Digital Markets Act), combating financial crime and terrorist financing



(EU Regulation on preventing the use of the financial system for the purposes of money laundering or terrorist financing – “AMLR”). DPAs are also playing a prominent role in matters related to cyber and data security. Said matters highlights the growing relevance of DPAs in a complex and evolving regulatory landscape.

Artificial Intelligence (“AI”).

AI was a central topic, with significant developments such as the EU AI Act and progressive and meaningful guidance from regulators such as the UK Information Commissioner’s Office (“UK ICO”), serving as important reference points in shaping data protection frameworks around AI. However, a point for reflection emerged: while substantial resources are being directed toward training

AI systems, is there comparable investment being made in education society about the importance of privacy and the principles of responsible AI? Ensuring public awareness and understanding is essential to building trust and fostering a culture of accountability as AI becomes more integrated into everyday life.

The Central Role of Data in Healthcare.

Another important discussion concerned the central role of data in the development of healthcare, where strong data protection and governance are essential for enabling better policymaking, improved care and fostering public trust. Key considerations include the lawful basis for processing and the distinction between primary and secondary uses of data.

Anti-Money Laundering (“AML”) and Data Sharing. This session explored developments encouraging both public – private and private – private data sharing to support efforts in combating financial crime and terrorism. It highlighted the critical role of data to combat financial crime and terrorism, while also stressing the need for strong governance frameworks to ensure data sharing takes place in a compliant manner.

15 May 2024 – ICO-OFCOM ECDPA Side Event on Age Assurance

The Division attended this ECDPA side event in Latvia, hosted jointly by both the ICO and Ofcom - the UK’s regulator for online safety – which focused on the ongoing collaboration between both regulators on age assurance. Key discussions highlighted the challenges that organisations face when implementing age assurance technologies and the regulatory responses provided to address these issues and any developments. Additionally, the event emphasised the importance of international collaboration to address age assurance concerns on a global scale.

14-15 May 2024 – National Cyber Security Centre (“NCSC”) CyberUK 24

The theme of this year’s NCSC conference, “Future Tech, Future Threat, Future Ready,” focused on the opportunities and challenges presented by emerging technologies. As technology rapidly evolves, adversaries, including cybercriminals, can exploit these developments. The conference highlighted the need to ensure that the data protection ecosystem remains resilient and prepared to tackle these evolving threats. Some of the sessions attended are summarised below:

Event Opening and Global Leadership

The conference opened with the NCSC’s CEO Felicity Oswald OBE addressing the growing threats, including AI advancements, the race for quantum computing and cryptography, and rogue state actions, particularly from China, Russia, Iran, and North Korea. She highlighted the publication of new guidance on ransomware, developed with the insurance industry, urging victim organisations to review it before paying ransoms. The importance of becoming “future ready” through collaboration, sharing expertise, and building stronger partnerships was emphasised. A

panel discussion covered the rise in attacks on supply chains and Critical National Infrastructure (“CNI”), as well as the evolving role of the internet, from a sharing platform to a tool for misuse. Automation technology was deemed essential to counter these emerging threats.

Building a Workforce of the Future

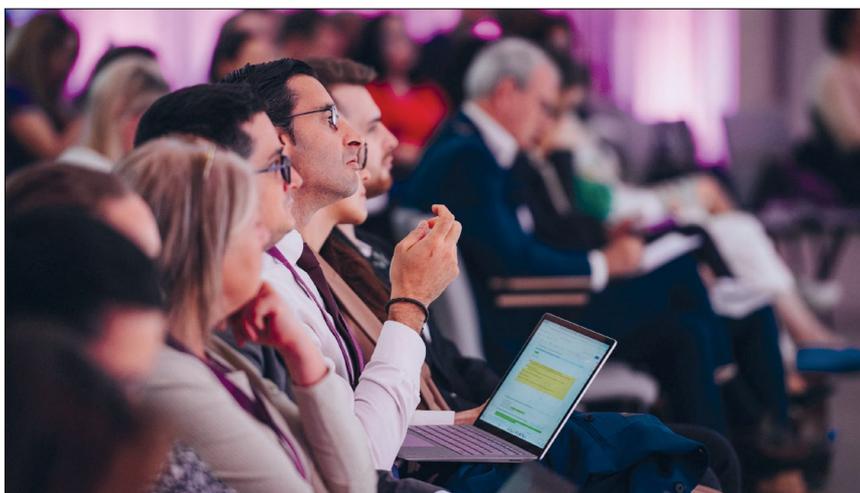
Led by Chris Ensor OBE, Deputy Director for Cyber Growth at NCSC, this session discussed the global challenge of building a skilled cybersecurity workforce. The panel explored how humans and AI can collaborate in the future-ready workforce, emphasising the need for industries to prepare for innovation. The UK Government’s adoption of the Cyber Security Council’s standards was announced to build trust in AI technology by incorporating core requirements like governance and secure testing. The ICO shared its use of AI in chatbots for handling helplines and complaints, demonstrating practical applications of AI in cybersecurity.

Incident Management

The NCSC-led session featured panellists from both public and private sectors who discussed the most innovative and impactful tactics that their Incident Management teams had to address this year. The NCSC’s ‘Early Warning’ system was also promoted, sharing positive outcomes from the past year and the concept of Advanced Persistent Threats (“APT”), were also explained. APTs were defined as persistent, patient, strategic and selective.

Biggest Hack Ever

This session, featuring investigative journalist Geoff





White, explored the intersection of technology, money laundering, and cybercrime. White discussed a hack on a Vietnamese video game that involved celebrities like Jimmy Fallon and Kim Jong Un, and the US government's fight over freedom of speech and cryptocurrency. White's research detailed how skilled cyber attackers often lack expertise in laundering the proceeds of their crimes. The session also examined the innovative ways attackers use publicly available online tools to evade detection, culminating in a stunning \$625 million heist that took just 1 minute and 33 seconds.

Cyber Proliferation

A panel led by Paul Chichester MBE, the Director of Operations at NCSC, discussed the growing threat of cyber proliferation with insights from government, industry and civil society. Key concerns included the 'zero-day economy' and the threat from spyware, particularly through vendors. The panel emphasised the importance of collaborative efforts to tackle cyber threats, acknowledging that costs will rise for those who fail to address these issues. Despite the challenges faced, the session concluded with an optimistic view on the need for ongoing cooperation to ensure future success in cybersecurity.

AI and Cyber Threats

In this session participants explored the impact of AI on cybersecurity, both for offensive and defensive strategies. It was agreed that whilst AI can be valuable in cybersecurity, it can also be leveraged by attackers, emphasising the need for layered defence to counter these risks. The panel also noted that many AI systems are designed for performance, not security, and can be manipulated for misinformation and disinformation. Securing supply chains and forming international partnerships and agreements were highlighted as essential steps.

17-19 June 2024 – 73rd Meeting of the International Working Group on Data Protection in Technology ("IWGDPT")

The IWGDPT observes trends and developments in technology, drafting recommendations and guidelines for the use of

emerging technology in a way that ensures data protection compliance. Also known as the 'Berlin Group', the working group is supported by Data Protection Commissioners and independent experts worldwide to improve privacy and data protection in technology.

Held in Oslo and hosted by Datatilsynet Norway, the DPA in Norway, the focus of the meeting revolved around the wider use of road charging, including sensory technology called "AutoPASS". The primary purpose for this system is to generate funding which is also deployed in trams and subways, to finance the planning and construction of public roads. Various data protection concerns were raised, including the collection, storage, and sharing of data related to the system.

The need to simplify cross-border travel by enabling billing across nations, adding that different technologies are already used to collect data on vehicle usage for fee calculation (e.g., CEN DSRC tags) was also discussed. A presentation outlined the various security standards followed to ensure compliance with international data protection regimes.

IWGDPT Topical Papers

The 'Data Sharing' and 'Large Language Model' ("LLM") papers were revised by all members



and were adopted following this session. These papers are published on the IWGDPT website alongside other recent publications, including Facial Recognition and, Central Bank Digital Currencies. New papers are being considered for next meetings relating to Emerging Neurotechnology and Data Protection and Extended Reality (XR).

1-3 July 2024 - Privacy Laws & Business 37th International Conference

This year's conference, held in Cambridge, UK, was titled 'Valuable Data, Priceless Privacy' and focussed on the tension between monetising data (i.e., the metric of data in money terms) and the abstract value of privacy, which is recognised by everyone but cannot be valued. Practical sessions covered topics on surveillance and facial recognition, international data transfers, children's and women's issues, data monetisation, using AI in different contexts, 'Privacy by Design', creating privacy notices, and AdTech. Summaries of some of the sessions attended by the Division are provided below:

Valuable Data, Priceless Privacy, Decaying Democracy

The session related to the relationship between data, privacy and democracy. Amongst the topics discussed were the importance of data protection and privacy for democratic rights, the significance of the work done by data protection authorities in promoting democratic rights, the digital campaigning environment in the UK elections of 2024 and the impact of AI on elections.

Regulating AI

The session focused on how privacy rights are "becoming commercial and technological assets which have an enormous impact on markets and geopolitics," according to Mr Guido Scorza, a Board Member of Italy's Data Protection Authority, the Garante. Speaking in his personal capacity, the session covered how according to Mr Scorza, data that is publicly available online should not be used to train algorithms. The session also covered how the Garante will continue its investigation into Open AI, even if temporarily stopping its processing was an unpopular decision for Italian consumers. While not wishing to stop innovation, Mr Scorza said that the Garante will try to act as fast as possible on AI questions. However, he also stressed that sometimes this meant making mistakes. He also stressed the role of education in the process.

A second session further explored AI and regulation. It consisted of a mix of question-and-answers with representatives from both industry and regulators, as well as the showcasing of a real AI experience. The topics raised included how, with the influx of regulation, businesses conceptualise calls for increased regulation, given that AI is developing very quickly. It was stated that amongst other things, regulation is a response to uncertainty, but development may be slowing down due to regulation. Equally, it was also stated that there are many benefits to AI, however many risks remain such as risks to privacy, copyright, disinformation and HR violations.

Cross-Regulatory Cooperation: Collaborating at the Intersections

The panel discussed the challenges that data protection authorities face when collaborating with other regulators outside of the privacy sphere. Panel members each discussed how their respective authorities achieve such collaboration, including through the creation of task forces, joint investigations, memorandums of understanding and where relevant, work with provincial partners. Amongst the challenges identified by the panel were the fact that laws may not be consistent within jurisdictions.

Regulators Tackle Children's Issues from Different Angles

The panel discussed how children's issues can be tackled from different angles. In this regard, the panel explained the role of enforcement, specifically discussing recent regulatory decisions and fines issued to Instagram and TikTok, as well as the importance of empowerment through education and outreach efforts. The panel also addressed the industry's role in protecting children online, highlighting that any impactful strategy needs participation from every key stakeholder i.e., businesses, children, educators, regulators, etc.

Optimising Data Monetisation Strategies Through the Use of Privacy-Enhancing Technologies

The panel considered the ways in which data monetisation strategies can be optimised using privacy enhancing technologies ("PETs"). The discussion focussed on the importance of data mapping, successful collaboration

between data governance and information security teams, upskilling the workforce to use PETs, understanding the legal framework and embedding privacy into data governance and data management systems, as well as articulating data ethics into strategies.

Tackling the Online Invasion of Women's Privacy

The panel discussed how the law is tackling the invasion of privacy in the context of increasing online threats of sexual violence, cyberstalking, intimate image release and deepfakes. The panel discussed the fast pace at which technology is moving and how the law is responding to address associated risks, including developments in criminal law that now make such acts easier to prosecute in the UK, the onset of the UK Online Safety Act 2023, the role of data protection, as well as the need to educate the public and reduce stigma.

Training AI Models While Protecting Privacy

The panel discussed how to train AI models while protecting privacy, highlighting the importance of having clear and robust settings for users, transparent explanations about the processing of any personal data and associated risks, as well as safety testing and measures designed to minimise bias and promote accuracy.

Aligning EU and UK GDPR Strategies

The session considered areas of divergence between the UK GDPR and the EU GDPR. The panel discussed topics such as the age of consent, the exclusion of the 'one-stop-shop' mechanism from the UK GDPR, the role and base of EU representatives and DPOs, international transfers, and the

impact of Brexit on the role of the ICO on the EU platform.

When a Data Processor Becomes a Data Controller

The session considered the roles of data controller and data processor, identifying the ways in which there could be a blurred relationship in practice and how this may be dealt with. The panel discussed topics such as how much discretion processors have before they become data controllers, retaining data processor status when using customer data for product improvement, what data a processor can use for machine learning and AI development, and how data controllers can protect themselves whilst benefiting from a data processors' initiative.

Designing for Cookie Compliance in a Changing Landscape

The session considered cookie compliance in a changing landscape and in the context of cookie-related enforcement action being carried out in the EU and the UK. The panel discussed the legal framework and relevant legislative provisions, including the requirements of valid consent and transparency, and how this can be reflected in cookie practices. The panel also considered the perceived shift away from using cookies.



9 July 2024 – Global Privacy Enforcement Network Sweep (the "GPEN Sweep")

GPEN was established in 2010 by the Organisation for Economic Cooperation and Development (OECD), and it promotes international cooperation among privacy regulators. This year's GPEN Sweep involved 26 privacy enforcement authorities reviewing over 1000 websites and mobile apps, uncovering widespread use of deceptive design patterns that make it difficult for users to make privacy-protective choices.

Deceptive design patterns, also known as "dark patterns", manipulate users into sharing more personal data by making privacy settings hard to access, using emotionally charged language, or repeatedly



prompting users to reconsider privacy decisions. For the first time, the GPEN Sweep was coordinated with the International Consumer Protection and Enforcement Network (ICPEN), recognising the increasing overlap between privacy and consumer protection.

In the case of deceptive design patterns, it was clear to both privacy and consumer protection sweepers that many websites and apps employ techniques that interfere with individuals' ability to make choices that best protect their privacy or consumer rights. The findings highlighted concerns over confusing privacy policies, interface designs that push less privacy-friendly choices, and obstacles preventing users from managing their data easily.

Although the GPEN Sweep was not a formal investigation, its results may lead to follow-up actions, including outreach to organisations or enforcement measures. GPEN encourages businesses to adopt transparent and user-friendly privacy practices, such as clear language, easy-to-access settings, and default privacy protections. By prioritising user trust and informed decision-making, organisations can enhance their reputation while ensuring compliance with privacy standards.

1 August 2024 – Digital Education Working Group (“DEWG”)

The DEWG, a sub-group of the Global Privacy Assembly (the “GPA”), focuses on data protection in education, particularly digital learning. With technology playing a growing role in schools, including in

Gibraltar, the Division actively contributes to discussions, trends and recommendations via online seminars and videocalls. Work is progressing steadily, with input from multiple DPAs, including updates on various multi-jurisdictional projects, some led by our Division. Discussions focus on key topics such as age assurance mechanisms to verify children's online access, strategies to support children in navigating digital environments safely, and resources for parents and educators to enhance digital literacy and privacy awareness. The Division plays a key role in the following international projects:

Teacher's Survey on Personal Data Protection and Digital Citizenship

This initiative aims to identify trends in teachers' relationship with personal data protection and digital citizenship. In doing so, the taskforce aims to assess current knowledge levels, common teaching practices, the perception of students, the availability and use of resources, and key training needs, amongst other matters.

Supporting Parents in Digital Literacy and Promoting Positive Parenting

Working as part of an international task force to meet the socio-educational challenges faced by digital technologies, with the aim of making it easier for families to understand the digital environment, the importance of autonomy, evolving capacities and the safety of the online environment whilst respecting the interests of the child.

Additionally, the Division has actively contributed to an awareness raising booklet led by the DEWG, titled “The

Importance of Personal Data and How We Protect It”. This booklet aims to highlight awareness initiatives undertaken by participating DPAs with young people, teachers and the public. Although published in the last quarter of 2024, the booklet covers activities carried out during the 2022-2023 period. Some of the topics covered within relate to the development of educational resources, physical awareness-raising events and fun days, social media campaigns, surveys and studies, competitions, and the creation of new platforms to further engage the public.

The Division is proud to have contributed to this initiative, with its work being well-represented and receiving significant international recognition. This acknowledgement reinforces the value of the Division's efforts in promoting data protection awareness and makes its participation in the working group especially rewarding.

26-27 September 2024 - British, Irish and Islands Data Protection Authorities (“BIIDPA”)

BIIDPA in-person meetings, which are held annually, provide participating DPA's with an opportunity to discuss topical matters in a smaller, close-knit forum. This year's meeting, held in Larnaca, Cyprus, saw participation from multiple DPAs including Bermuda, Cyprus, Gibraltar, Guernsey, Ireland, Jersey, Malta and the UK.

BIIDPA DPAs have a longstanding and close relationship, which involves routine collaboration on key matters with DPAs leveraging on each other's experiences, resources and competencies to create synergies and maximise

capabilities. This year's meeting discussed key developments and ideas in several areas, such as:

Competences, Structure and Resources

Participants highlighted the challenges and varying approaches used in different jurisdictions to facilitate efficient and effective regulation, such as outcome-based regulation which focuses on achieving specific objectives rather than prescribing detailed processes. They discussed how this approach allows for greater flexibility and adaptability in responding to evolving technologies and regulatory landscapes.

The Challenges of Day-to-Day Supervision

This session highlighted the growing complexity of the data protection landscape, particularly as it intersects with various laws, regulations and rapidly advancing technologies. This convergence of differing legal frameworks creates additional challenges for organisations attempting to navigate compliance requirements. The session underscored the critical importance of international and sectoral cooperation in addressing these challenges, with participants recognising that global collaboration is essential for creating cohesive and effective solutions across borders.

The Role of the DPO

The challenges faced by DPOs were discussed in detail, drawing from the unique experiences and perspectives of each jurisdiction represented. The discussions highlighted the various hurdles DPOs encounter

in their roles, such as navigating complex legal frameworks, ensuring compliance with evolving data protection laws and managing the increasing volume and complexity of data across organisations. Other conversations explored the practical difficulties DPOs face in educating and training staff, implementing effective data protection measures and maintaining ongoing oversight of data handling practices. Ideas for improvements were put forward to address these challenges, including the development of more standardised processes and clearer guidelines to streamline compliance efforts.

AML/Counter Terrorism ("CT") and Data Protection

The growing intersection of legislation, including developments in information sharing and opportunities for collaboration with sectoral regulators and stakeholders, presents both challenges and opportunities for strengthening the effectiveness of AML and CT measures alongside data protection frameworks. This evolving landscape calls for closer coordination between regulators to ensure that data privacy is maintained while enabling the efficient exchange of critical data to prevent illicit activities.

Secondments

Opportunities for secondments were discussed and jurisdictions shared recent examples and experiences that have allowed DPAs to leverage on each other's expertise and resources.

Cookies

Cookies have become a significant area of focus in recent regulatory discussions,

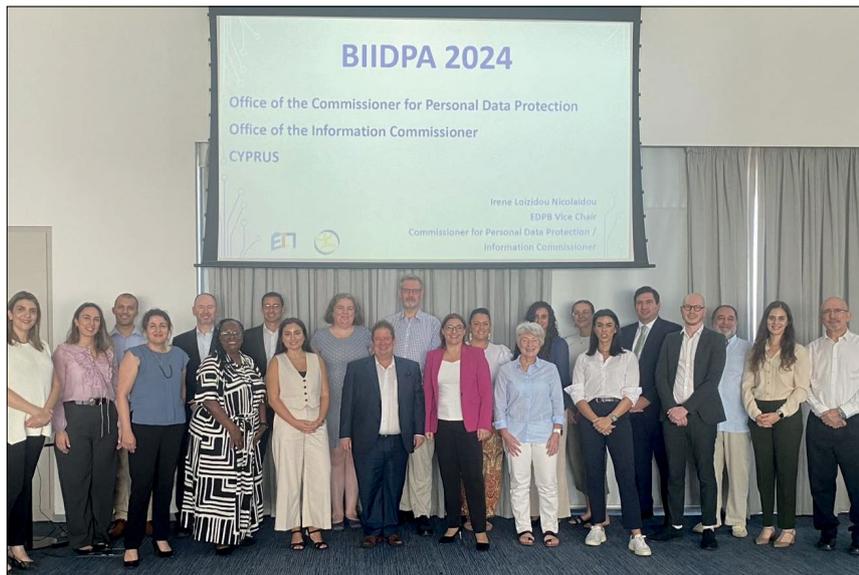
with ongoing work aimed at addressing the evolving challenges related to their use in the digital ecosystem. This includes concerns about user consent, transparency, and the impact of cookies on privacy rights. Recent regulatory developments highlight the need for clearer guidelines on how organisations should inform users about the use of cookies, obtain valid consent, and provide mechanisms for users to manage or opt-out of cookie tracking. This area of focus is expected to evolve further as new technologies emerge and more stringent privacy regulations are enforced.

Public vs Private Sector Compliance

During the session, participants shared their experiences regarding public and private sector compliance, highlighting common issues such as differing regulatory approaches, resource constraints, and challenges in aligning data protection practices across both sectors. These discussions emphasised the need for a unified approach to compliance, where both sectors can learn from each other and collaborate on best practices to address overlapping concerns such as risk management, data security, and regulatory adherence.

Minors' Privacy

Minors' privacy has increasingly become a focal point in recent data protection discussions, with both regulators and industry stakeholders placing significant emphasis on safeguarding the personal data of children and young people in the digital space. A joint statement on age assurance, issued by leading regulators, underscores the importance of developing and



implementing effective age verification technologies to prevent minors from accessing content or services that may not be appropriate for their age group. Further details on this topic will be provided later in the report.

4 September 2024 – Global Privacy Assembly International Enforcement Working Group (“IEWG”) Capacity Building Workshop

Capacity Building Workshops provide DPAs, with a forum for exchanging experiences and perspectives on topics of particular interest that may influence their operational activities. In September 2024, the Division participated as a panellist for the virtual workshop on ‘Complaint Handling’, which was moderated by the Office of the Privacy Commissioner of Canada. Other panellists included the ICO and the CNIL.

In this workshop, panellists with different legal frameworks and resources shared corresponding challenges, as well as potential solutions and tools to improve and adapt complaint management strategies. These discussions focused

on processes and structures implemented to efficiently triage an increasing number of complaints, addressing lower risk complaints outside of a comprehensive investigation, and tackling complaint backlogs. The collaborative nature of the workshop fostered insightful discussion into best practice approaches for complaint handling.

1 October 2024 – Global Privacy Assembly IEWG Capacity Building Workshop – Public Awareness and Promoting Compliance

The Division attended an IEWG online workshop moderated by the Norwegian DPA. The workshop provided an open platform for discussion and collaboration between participating DPAs, allowing them to exchange insights, best practices and challenges when embarking on awareness-raising initiatives. A common theme throughout (and particularly for larger countries) was the challenge of properly communicating the importance of data protection and privacy matters. This was particularly troublesome for countries that had remote areas with limited

or no access to the internet or news outlets. Participants also discussed the difficulty in striking the right balance between privacy awareness engagement and the undertaking of more formal work such as enforcement action.

This collaborative environment encouraged constructive dialogue on regulatory approaches, and emerging privacy issues, fostering a shared understanding of how best to address awareness-raising initiatives and public engagement across communities.

25 October 2024 – Joint Statement on the International Approach to Age Assurance

The Division’s work includes engaging with data protection and privacy authorities globally (“Global Authorities”) to protect children, and particularly their personal data, online. Channels used to foster such international engagement include the International Age Assurance Working Group (“IAAWG”).

Through the IAAWG, several Global Authorities have jointly drafted a statement promoting a unified international approach to age assurance. This statement outlines shared principles and outlines the common goals and commitments from signatory regulators including: the ICO, the National Privacy Commission of the Philippines; the Office of the Privacy Commissioner of Canada; the Public Information Access Agency from the National Authority for Personal Data Protection in Argentina; and the Transparency, Public Information Access and Personal Data Protection Institute of the State

of Mexico and Municipalities.

The Division anticipates that this work will encourage increased policy coordination internationally and improved regulatory clarity for relevant stakeholders in relation to the use of children's personal data.

28 October – 1 November 2024 – Global Privacy Assembly (“GPA”)

The Division attended the annual GPA, the premier global forum connecting the efforts of more than 130 DPAs worldwide. Industry and civil societies also joined the event to contribute and deliberate on key discussions and developments.

The conference, held in Jersey, was centred around the theme “The Power of I”, reflecting a broad spectrum of key concepts, including Individuals, Innovation, Information, Integrity, Independence, International, Intercultural and Indigenous. The following outlines some key matters discussed and/or highlighted during the weeks discussions –

Individuals and Information

Protecting Children. The GPA placed a strong emphasis on the risks technology can pose to children, highlighting the urgent need to safeguard their rights in the digital age.

Giving Children a Voice. A panel of schoolchildren at the GPA shared their perspectives, acknowledging the benefits of technology while expressing concern about its impact on freedom, privacy, and personal and social development. The children called for greater accountability from major tech companies and emphasised the importance of privacy education.

DPA Initiatives. GPA members discussed work done by DPAs across the globe, which centred on the promotion of EdTech compliance, raising privacy awareness amongst children and upholding children's information rights. Further information provided under the section titled “GPA's Digital Education Working Group (“DEWG) and UNICEF: Workshop on Children's Data in EdTech”.

Prioritising the Vulnerable

The GPA emphasised the importance of a human-centric, risk-based approach to data protection — one that places the most vulnerable at the forefront. Key points highlighted were - 1) In humanitarian settings, data protection is not just a legal or ethical concern — it can be a matter of life and death. Discussions highlighted the critical role of the International Committee of the Red Cross' 3rd edition Handbook on Data Protection in Humanitarian Action as a

key resource; 2) data breaches can have disproportionately severe emotional impact on individuals with mental health conditions 3) a seemingly minor administrative error can have serious consequences — for example, exposing the confidential address of someone who has recently escaped an abusive relationship.

New Zealand's Information Commissioner powerfully captured a human centric ethos by referencing a Māori proverb: “What is the most important thing in the world? It is people, it is people, it is people.”

Innovation

Innovation was a central theme in the GPA discussions, which recognised emerging technologies such as AI and immersive tech as key developments that represent significant progress, but which also introduce new risks that must be addressed. The message was clear: “Prepare today for a better tomorrow” and “By failing to prepare, you are preparing to fail”.

Innovative regulatory approaches are essential for keeping pace with technological advancements. Initiatives such as regulatory sandboxes and CNIL's Digital Innovation Lab were highlighted as proactive examples helping to guide responsible innovation.

Further, the importance of recognising and incentivising Privacy Enhancing Technologies (PETs) was also emphasised. The International Working Group on Data Protection in Technology has contributed to this discussion through its working papers on Central Bank Digital Currencies and Facial Recognition Technology. In addition, the Council of Europe's



work on neurotechnology was noted—particularly a scientific report by Eduardo Berton and Marcello Lenca, which explores the privacy and data protection implications of neurotechnology and neural data under Convention 108+.

Integrity & Independence

The historical shift in power from ruling elites to the people stands as one of the most transformative innovations in human history. It laid the foundation for a rights-based, rule-governed order that supports transparency, fair trade, and thriving economies.

At the heart of this transformation lies the principle of independence, particularly for regulators tasked with upholding the rule of law. Independent institutions are essential to ensure impartiality, credibility, accountability and trust, which are ever more important in an increasingly data-driven world. The integrity and independence of regulatory bodies are not just ideals — they are cornerstones of effective governance, societal resilience and long-term success.

International & Intercultural Cooperation

The discussions highlighted the significance of developing international standards that are mindful of diversity — recognising that cultural, economic, developmental, and

legal contexts vary, and that a one size does not fits all.

Further, a strong theme emerged around collaboration, summed up by the sentiment: “Alone we can do so little; together we can do so much.”

In the financial services space, international data flows were highlighted as essential. The Director for Information Rights and Operations, Bradley Tosso, participated in a panel on cross-border payments with Bermuda’s Commissioner Alexander McD White, the Dubai International Finance Centre’s VP for Data Protection Lori Baker, Singapore’s Personal Data Protection Commission’s Deputy Commissioner Denise Wong, and the Financial Action Task Force’s President Elisa de Anda Madrazo. The panel emphasised three key points: 1) the close link between data privacy, trust, and finance; 2) the role of innovation-enabling initiatives; and 3) the critical importance of cooperation between data protection authorities, financial regulators, and industry stakeholders.

Indigenous Communities

The GPA’s discussions highlighted the importance of promoting and/or ensuring an inclusive digital journey ahead. Communication strategies and technological development should actively consider the unique needs of indigenous

communities. While the application of data protection may differ across various contexts, a universal principle remains: the respect for each individual and their dignity—as noted by Massimo Marelli, Head of the Data Protection Office at the International Committee of the Red Cross.

31 October 2024 – Memorandum of Understanding (“MoU”) with the Jersey Data Protection Authority

The GRA and Jersey’s DPA signed an MoU, which underlines the mutual commitment to further strengthen cooperation between both regulators. The formalisation of the relationship will serve not only to reinforce existing ties, but to also build upon capacity building and joint efforts in areas of common interest and concern.

Jersey’s Information Commissioner Paul Vane commented: “The signing of this MoU reinforces the joined-up approach between our two jurisdictions, strengthening cross-border collaboration in the interests of our Jersey and Gibraltar communities.” Gibraltar Information Commissioner John Paul Rodriguez commented on the importance of international cooperation, noting “cooperation facilitates a more efficient and



effective approach to regulation, particularly in the context of ever-increasing complexities in technology and globalisation”.

31 October 2024 – GPA’s Digital Education Working Group (“DEWG) and UNICEF: Workshop on Children’s Data in EdTech

The event hosted by the DEWG and UNICEF, addressed the importance of protecting children’s data in EdTech. The event underscored the global need for robust data governance, improved transparency, and stronger safeguards to protect children’s personal information in the expanding EdTech sector. Some of the key initiatives showcased during the workshop, included:

1) The EdTech Privacy Charter for Schools (Ontario).

Ontario created a Digital Privacy Charter for schools, which aims to protect student privacy, enhance accountability, and build digital citizenship. A voluntary pledge supports children’s rights in the digital space.

2) Supporting responsible innovation e.g. Education Credential Sandbox (UK).

The ICO discussed its work with the UK Department of Education, which involves the concepts of decentralised identity and verified credentials to allow post-16 students within the English education system to access, control and use their own personal data when applying and enrolling into further education organisations, via the use of an education credential.

3) Strategic partnerships (GPA and UNICEF collaboration).

The importance of forming partnerships that will foster synergy and amplify impact on both regional and global scales.

4-6 November 2024 – 47th Plenary Meeting of the Consultative Committee on Convention 108: Convention for the Protection of Individuals with regard to Automated Processing of Personal Data (“C108”)

The Division attended the 47th annual meeting of the C108, held in Strasbourg. As the only legally binding international instrument on the protection of personal data, with 55 parties and 25+ observants, C108 has two main aims: workings towards the free flow of data and the upholding information rights in accordance with the only legally binding international instrument in the data protection field.

Parties to C108 are required to take the necessary steps in their domestic legislation to apply the principles it lays down to ensure respect in their territory for the fundamental human rights of all individuals with regard to processing of personal data.

Whilst its core principles remain, the C108 was modernised in

2018 to create Convention 108+ (“C108+”). The modernisation pursued two main objectives: to deal with challenges resulting from the use of new information and communication technologies and, to strengthen the Convention’s effective implementation. Some of the key topics discussed are outlined below:

Transborder data flows of personal data: focusing on Model Contractual Clauses (“MCCs”), interoperability and other possible tools, including adequacy mechanisms; the EU-US Data Privacy Framework; appropriate safeguards (Binding Corporate Rules, Standard Contractual Clauses, Code of Conducts and certifications; tailor-made contractual clauses; and APEC Cross Boarder Privacy Rules Systems Programme.

Privacy Enhancing Technologies (“PETs”) as discussed in a presentation delivered by Prof. Chris Russell of the University of Oxford. This session looked at privacy and data protection considerations in the context of federated machine learning and LLMs.

Cooperation with other Council of Europe Bodies and Entities

This session included work with the Committee of Human Rights in the field of biomedicine and



health and the Committee on AI (“CAI”). CAI developed an international convention which is a mutually binding legal framework and is the only international legally binding framework on AI.

As AI technology transcends borders, the goal is for CAI to become a global instrument, including aspects related to cybercrime and data protection. The CAI and C108+ committees aim to collaborate, ensuring expert exchanges and synergy. While C108+ applies to both public and private sectors, its enforcement remains the responsibility of individual states, reinforcing that human rights extend beyond governments to all citizens.

5-6 December 2024 – European Case Handling Workshop (“ECHW”)

The ECHW is a forum for participative dialogue among DPAs on the challenges they are confronted with and the solutions they apply in their day-to-day practice. This year it was organised by the Estonian Data Protection Inspectorate in Tallinn, Estonia where topics such as the use of CCTV, data protection impact assessments (“DPIAs”), new technologies, information security and data breaches, AI governance and the role of DPAs, as well as the relationship between data controllers and data processors were discussed. Summaries of the key sessions attended are provided in the following:

CCTV

This session concerned the domestic use of CCTV, specifically individuals operating their own CCTV cameras on their private property, including

CCTV set up by residential/housing committees. A discussion ensued on the need to find a balance between two competing interests, namely an individual’s right to safety and security of their property and the protection of privacy.

Most DPAs acknowledged that the use of CCTV continues to increase as do complaints in respect of the same. The main areas of concern included the lawfulness of installations, a lack of transparency, and inadequate security.

With regards challenges to the resolution of such complaints, DPAs identified a lack of resource, inadequate legislative frameworks, public misunderstanding, and a lack of cooperation as the main contributing factors. With regards ways to manage and address these challenges, the session highlighted the need to raise awareness about the potential privacy issues, as well as the benefits of focussing on amicable resolution between parties and implementing a “soft” approach such as issuing letters of recommendation with guidance and information regarding the consequences of a breach of the law.

The session also considered the broader social impact of CCTV, including ‘smart’ CCTV, and whether DPAs should be doing more, such as collaborating with law enforcement, residential/housing committees, manufacturers, etc.

Data Protection Impact Assessments (“DPIAs”)

The session highlighted the benefits of undertaking DPIAs as enhancing compliance with data protection law, identifying and mitigating potential risks, improving information

governance, building trust, and promoting better decision-making. DPAs acknowledged that DPIAs act as a vital safeguard and necessary step for responsible innovation. However, the challenges of carrying out a DPIA were also identified, including that they are resource intensive. In this regard, the session also considered the potential difficulties of conducting a DPIA on AI models. Discussions revolved around their complexity and lack of standardisation, lack of transparency, potential biases, as well as the evolving nature of the technology and legal requirements.

In the context of AI models, the session highlighted the importance of including clear and detailed descriptions of such models within a DPIA, including their purposes, the types of data processed and how these operate, as well as the need to sufficiently assess measures designed to provide transparency, and minimise bias and promote accuracy.

New Technologies and Information Security; Data Breaches

This session considered DPAs’ processes for assessing a personal data breach notification (“Breach Notification”) including challenges faced and areas requiring development to improve the same.

DPAs acknowledged that challenges stem from both the complexity of the data protection landscape, internal constraints, as well as the nature of the breach themselves. DPAs highlighted the scale of impact, technological complexities, availability of evidence, organisational preparedness, and evolving guidance as the

main factors impacting their ability to progress and maintain timescales for the handling of Breach Notifications.

In addition, DPAs acknowledged the following as internal issues affecting efficient Breach Notification handling: limited resources in the context of a growing number of Breach Notifications; navigating different legal frameworks and protocols in the context of cross-border breaches; the need to strike a balance between regulatory enforcement and guidance; and the need to balance transparency to maintain public trust in the regulatory process with the protection of affected individuals' privacy.

DPAs identified the following as priorities to address the above-mentioned challenges: having a simplified notification system that provides relevant guidance and checklists; reviewing strategic objectives and integrating these into the triaging process, for example, focussing on harmful impact on individuals, including vulnerable groups; providing first-line response teams with cyber training and investing in prioritisation assessment tools to ensure escalation of cases as appropriate; investing in tools that provide shared workspaces for live collaboration; and

engaging with the cybersecurity community to leverage further expertise and promote a collaborative approach to data protection.

28 January 2025 – Computers, Privacy and Data Protection (“CPDP”) Conference

CPDP is a non-profit platform originally founded in 2007 and has since grown into a platform carried by 20 academic centres of excellence from the EU, the US and beyond. As a world-leading multidisciplinary conference, CPDP offers the cutting edge in legal, regulatory, academic and technological developments in privacy and data protection.

The Division attended the second edition of CPDP Data Protection Day, co-organised by the CPDP, the Council of Europe and the European Data Protection Supervisor (“EDPS”). The event attracted around 400 in-person attendees and hundreds more online, with speakers from 37 institutions, universities, and organisations.

The sessions highlighted key themes of continuity and adaptation in data protection. While new mandates are shaping policies, the event emphasised the ongoing role of data protection in safeguarding

democracy and the strength of existing institutions in enforcing regulations. Discussions also touched on the future of the GDPR and the evolving role of C108+ as a global standard for data protection. The conference also acknowledged the persistent challenge of legislation lagging technological advancements. While neuroscience and data protection were discussed in depth, issues related to quantum technologies were not a central focus despite their growing relevance. Additionally, concerns were raised about the complexity of EU digital legislation, with industry voices agreeing that regulations remain difficult to navigate, even for experts.

A key takeaway was the need for multidisciplinary perspectives in data protection. Beyond privacy, data protection now intersects with democracy and fundamental rights, requiring input from various fields, including social sciences, to make laws more actionable and effective.

Local Collaboration

11 April 2024 – Data Protection Workshop for SMEs

As part of ongoing efforts to support data controllers and promote compliance with data protection laws, the Division, in collaboration with the Gibraltar Federation of Small Businesses (“GFSB”), organised a SME Data Protection Workshop, held on 11 April 2024.

The workshop focused on the importance of data protection



in today's digital business environment and covered four key areas:

The Importance of Data Protection

The session underscored the critical importance of data protection, highlighting the risks and potential harm posed by data breaches, regardless of an organisation's size. Discussions emphasised how strong data governance not only helps businesses safeguard sensitive information but also fosters customer trust and strengthens their reputation. Additionally, data protection was presented as both an investment and a competitive advantage, demonstrating how effective compliance strategies can save businesses time, money, and resources in the long run.

Accountability & Compliance

The session highlighted the principle of accountability as a cornerstone of ongoing compliance with data protection laws. It emphasised the importance of organisations demonstrating their commitment to data protection through proper governance and transparency. Practical guidance was provided on key accountability measures, including record-keeping, conducting DPIAs, and the crucial role of DPOs in ensuring compliance and mitigating risks.

The Role of DPOs

The session provided an in-depth look at the designation, responsibilities, and challenges of the DPO role under the Gibraltar GDPR and the DPA. It also examined key findings from a European Data Protection Board survey, which highlighted common challenges faced by DPOs across

the European Economic Area (EEA), offering valuable insights into best practices and areas for improvement.

The Rights of Individuals

The session outlined individuals' data protection rights and provided practical examples of how organisations should uphold them. It also included an interactive audio-visual segment focused on the Right of Access, featuring videos from the GRA's YouTube Channel to enhance understanding and engagement.



17 April 2024 – Remote Gambling Data Protection Workshop

The Gibraltar Betting and Gaming Association ("GBGA") organised a workshop to address sector specific data protection concerns within the remote gambling industry. The event featured presentations from the Division covering key topics,

including:

Targeted Social Media Marketing ("TSMM")

The session provided an in-depth analysis of data protection considerations for businesses engaging in digital advertising, particularly within the remote gambling industry. It emphasised the importance of determining the appropriate lawful basis for processing personal data under Article 6(1) of the Gibraltar GDPR and, where applicable, identifying the necessary conditions under Article 9(2) for special category data. Attendees were guided on the need to clearly define roles and responsibilities, particularly in distinguishing whether they act as data controllers or joint controllers when utilising TSMM tools.

A key focus was placed on user consent and the right to object to data processing for direct marketing purposes under Article 21 of the Gibraltar GDPR. The session explored best practices for obtaining valid consent, including adherence to the principles of transparency and informed choice, ensuring that users fully understand how their personal data will be used for TSMM campaigns.

Online Cookies

The session outlined the legal obligations businesses must adhere to when deploying cookies, emphasising the need for clear and comprehensive information to be provided to users before setting non-exempt cookies. It also covered the necessity of obtaining valid user consent, in accordance with the principles of transparency and informed choice, ensuring that users can easily opt in or withdraw consent at any time. Best practices were

shared, including strategies for implementing compliant cookie banners, designing user-friendly consent mechanisms, and maintaining records to demonstrate compliance.

Ransomware and Credential Stuffing Attacks

The session outlined the risks and mitigation strategies in relation to ransomware and credential stuffing attacks. It was noted that credential stuffing attacks exploit individual's tendency to reuse passwords, with large volume of compromised credentials being traded online for cybercriminal activity. Guidance published by the Division was highlighted and discussions about ransomware ensued, noting the growing trend of extortion-based attacks. Emphasis was placed on the need for organisations to mitigate cyber risks by implementing strong security measures in line with Article 32 of the Gibraltar GDPR.

AI from a Data Protection Perspective

The Director of Information Rights and Operations joined the GBGA's General Secretary for a discussion on AI and data protection, focusing on regulatory developments in Gibraltar and internationally. The session highlighted the need for AI controls to ensure safe and responsible use, as deficiencies can undermine consumer confidence and business competitiveness.

Key data protection principles from the Gibraltar GDPR were explored, including transparency, fairness, data minimisation, accuracy, and accountability. Bias in AI was a major concern, with recommendations for organisations to implement fairness evaluation measures and verify AI-generated content with

trusted sources. Data protection rights, such as access, the right to be informed, and rights related to automated decision-making, were also discussed, alongside the importance of DPIAs and integrating data protection from the start of AI projects.

The session examined different regulatory approaches, such as the EU's AI Act and the UK's sector-based framework and practical guidance. The Gambling Commissioner also shared insights on AI developments within the industry. Emphasis was placed on collaboration between businesses and regulators, encouraging gradual improvements over rushed changes to ensure compliance and innovation go hand in hand.



18 April 2024 - Gibraltar Regulators Forum – Meeting

The third forum meeting welcomed a new member to the forum from the Legal Services Regulatory Authority ("LSRA"). This aligns with the forum's objective and aim of increasing its membership from other regulatory authorities and bodies. As part of the agenda, each of the members were invited to offer updates within their areas. These updates included:

GRA – an overview of recent workshops organised in conjunction with the GFSB and

the GBGA was provided. The work carried out by the Division in this regard focused on delivering bespoke workshops for specific sectors in Gibraltar, delivering guidance on selected topics applicable to them.

Gibraltar Financial Intelligence Unit ("GFIU") – described their work with international bodies to counter AML and highlighted the value of Private-to-Private Partnerships and exchange of information.

Gambling Commissioner – explained one of his main areas of focus being preparations for the new Gambling Act and updating of their Remote Technical and Operating Standards.

Gibraltar Financial Services Commission ("GFSC") – discussed additional areas being considered that could fall under their regulatory responsibilities. This included consideration of possible regulatory challenges, brought about by new emerging technologies.

LSRA – explained their focus is on strategy and welcomed the acceptance of the LSRA as a member to the forum, recognising the value such alliance generates.

10 May 2024 – Data Protection Workshop for Charities

Funded by Kusuma Trust, the Division organised a bespoke data protection workshop for Gibraltar-registered charities. During the workshop, key data protection concerns, and compliance requirements were addressed, including:

Introduction to Data Protection

The session highlighted how advancements in digital

technology have increased personal data processing, emphasising the associated risks and potential harm from data breaches, regardless of the organisation's size. It stressed the importance of strong data protection measures to safeguard both individuals and organisations, particularly for charities with limited resources. Given their reliance on trust, donations, and long-term support, charities must prioritise data governance to maintain credibility. Real-life examples illustrated the consequences of data mismanagement and security breaches.

Lawful Basis for Processing Data

The session explained that organisations must have a lawful basis under the Gibraltar GDPR before processing personal data, with the appropriate basis depending on the purpose. Practical examples were provided, along with guidance on handling special category and criminal offence data. The importance of assessing risks appropriately was also highlighted.

Data Protection Principles

The session covered key data protection principles under Article 5(1) of the Gibraltar GDPR and examples specific to charities were used to illustrate these principles. Data controllers were also reminded about the importance of demonstrating compliance, as required by Article 5(2) of the Gibraltar GDPR.

The Rights of Individuals

In today's data-driven landscape, it is imperative that charities, like any other data controller, ensure that personal data is protected and processed in compliance with data protection

law. This session covered individual's rights focusing on access, information, erasure and rectification. Attendees learned about handling excessive or unfounded data subject requests through practical examples and an interactive activity encouraged discussion. The session concluded with insights on regulatory perspectives, highlighting the importance of an active approach to data protection.

Additional Considerations

The final session covered additional key data protection aspects, including data sharing, breach notifications, employment-related data and handling vulnerable individuals' data. The charities were advised to provide clear privacy notices and conduct DPIA's, where necessary.



25 May 2024 – Launch of the SME Resource Hub

25 May 2024 marked six years since the introduction of the

EU GDPR, which was replaced locally by the Gibraltar GDPR on 1 January 2021. The GDPR impacts SMEs and how they handle personal data, especially with the rise of new technologies.

To support businesses, the Division launched an SME Resource Hub, offering user-friendly guidance on data protection principles, managing breaches, and compliance best practices. Available via the GRA website, the hub provides resources in the form of infographics, social media campaigns and audio-visual content. By promoting responsible data handling, organisations can prevent cyber threats, maintain customer trust and ensure compliance. SMEs are encouraged to explore and share the resources to further strengthen privacy awareness across Gibraltar.

12 June 2024 – Gibraltar Regulators Forum – Ransomware Survey

The GRA, as part of the Gibraltar Regulators Forum, has launched a survey to assess the impact of ransomware attacks on Gibraltar and improve cybersecurity measures. Ransomware is a type of malicious software designed to block access to a computer system or data, often by encrypting the data, until a sum of money is paid. These attacks can be devastating, causing significant disruption to businesses and personal lives, as well as leading to financial losses and potential breaches of sensitive information.

Developed in collaboration with the forum's key regulatory bodies, the survey aims to identify the prevalence of ransomware incidents, evaluate security measures,

and enhance public awareness. The anonymous results will help shape strategies to protect individuals and organisations.

An update regarding the survey can be read below.

27 June 2024 - Virtual Workshop on Data Security Dialogues

The importance of cybersecurity continues to grow as the volumes of personal data processed increases (particularly in the online environment) and because malign actors become more sophisticated. The virtual workshop, organised by the Division, aimed to facilitate engagement between DPOs (and other relevant professionals) and data/cyber security experts/organisations. This initiative formed part of the Division's efforts to provide support and assistance to organisations on data protection risks and compliance.

The event was well attended and saw two organisations, Forensic Pathways and Thomas Murray (UK), present on emerging cyber security threats and tools available to mitigate/protect against said threats.

4 July 2024 - Gibraltar Regulators Forum – Meeting

The fourth forum meeting mainly focused on the Ransomware Survey which assessed the prevalence of ransomware attacks and cybersecurity resilience within Gibraltar. The GFIU led the meeting, with members discussing early survey findings and updates on response progress. The forum also continued work on the Ransomware Paper, with discussions centred on the draft



review process and expected publication in 2025.

Other key topics discussed included breach notification requirements and the development of a unified breach notification form as well as data sharing in AML/CFT whereby forum members explored ways to balance data protection with the need for effective information exchange in combating financial crime.

24 September 2024 – Island Data Governance Forum (“IDGF”) & GRA Data Protection Workshop

In conjunction with the Islands Data Governance Forum, the Information Commissioner hosted a Data Protection Workshop on 24 September 2024. Held at the Rock Hotel, this event covered a variety of topics including real-life implications of data processing, as follows:

Session 1: David Carney (IDGF Vice Chair) – What Does My Data Say About Me?

The speaker highlighted concerns regarding our privacy and how data is used in areas such as online accounts and CCTV systems. Aspects of security associated with the sharing of data was discussed, as was the importance of online

T&Cs which, if misunderstood or ignored, could make user vulnerable to threats such as ID spoofing and ‘weaponizing’ of their data through different means.

The speaker discussed the pros and cons of AI as well as the use of CAPTCHA and the ability of machine learning by data hungry collection, highlighting further risks about data collection, data inaccuracy and retention.

Session 2: Regulators Panel: Alan Pereira (GFSC), Bradley Tosso (GRA) and Francis Muscat (LSRA)

The panel brought together regulators from different sectors such as data protection, finance and legal services to allow for a more comprehensive understanding of issues that transcend individual regulatory domains. The panel highlighted the importance of cross-regulatory cooperation and discussed ongoing efforts regarding the consolidated data breach notification process and the ransomware project. The former process enables the simultaneous notification of a data breach to different regulators to enable coordination and ease regulatory reporting, and the latter project aims to identify the prevalence of ransomware threats across different sectors in Gibraltar.

Session 3: Stephen Green (Thomas Murray, UK) - The Cyber Landscape of Gibraltar

The speaker discussed the cyber landscape of Gibraltar and highlighted that the two main threat actors emerged from the geo-political spectrum and finance targeting, noting Gibraltar's prominence for cyberattacks given its interconnected technological and financial relationships with the UK and Europe. Cyberattacks such as hacktivist threats, distributed denial of service attacks (DDOS), ransomware, spear phishing and social engineering tactics, as well as supply chain threats and business email compromise were discussed.

Session 4: Ainhoa Gonzalez (Entain) and Joseph Gaunt (Evoke PLC) – Assessing and Governing AI from a Privacy Perspective.

Organisational AI governance was at the forefront of discussions. This refers to a set of rules, processes, and tools to ensure the ethical and responsible development of AI which, in today's digital environment, is rapidly becoming an essential tool to enhance efficiency. However, AI raises social and ethical responsibilities, which require governance measures including impact assessments. A governance framework is necessary, with cross-functional teams (legal, compliance, technology) to oversee AI across its development cycle. This includes crafting an AI Ethics Charter, conducting bias assessments, and ensuring continuous control over algorithms while fostering innovation.

Session 5: Laura Lewis (Rank Group) and Jade Smith (Sovereign Group) – A DPO's Perspective: Focusing on the Value of Data Protection

In the realm of data protection, a DPO plays a crucial role in an organisation in overseeing operations, ensuring compliance, and building strong relationships with key stakeholders. It's essential for a DPO to understand their role and risk appetite, while also recognising business priorities and previous practices. Speakers at this session discussed the importance of fostering partnerships through curiosity and open dialogue within the organisation. They described their core responsibilities to include monitoring compliance, conducting audits, raising awareness through training, acting as a liaison between the business, data subjects, and authorities, and providing guidance on risk management without making final decisions.

Session 6: Brent Horman (Office of the Data Protection Authority, Bailiwick of Guernsey) – GPEN Privacy Sweep: Dark Patterns in the Online Gambling Sector

This initiative, organised by GPEN, examined global privacy practices with a focus on dark pattern indicators like obstruction, sneaking, nagging, and forced actions (the "Sweep"). The Sweep's findings revealed issues such as complex privacy policies, opaque consent mechanisms, difficulty in finding deletion options, and challenges in selecting privacy-friendly settings. The Sweep also identified key improvements which included enhanced account deletion processes and more transparency in privacy settings. It was found that for online gambling companies, in particular, privacy is critical due to the high volume of sensitive data processed, regulatory scrutiny risks, and the need to build user trust.



Session 7: Data Protection Regulators Panel with Brent Horman (Office of the Data Protection Authority, Bailiwick of Guernsey) and Bradley Tosso (GRA)

This session included a fireside chat covering various aspects relating to data protection regulation, including international cooperation in the context of small jurisdictions. The panel discussed the impact of technology on the data protection landscape and how international projects into credential stuffing, for example, highlighted the growing concern of online security threats to individuals and organisations. To this end, the value of international cooperation was emphasised, showcasing how pooling resources and leveraging on the expertise of other regulators and stakeholders can compensate for resource limitations, enabling regulators to exceed their capabilities.

The panel acknowledged that when monitoring compliance, a proactive, incentive-based approach is preferred. They recognised the difficulties faced by DPOs, adding that there is a desire to incentivise and highlight exceptional DPOs, encouraging compliance and excellence in data protection practices.



25 September 2024 – Day in Town Event

With the rise of new technologies, organisations are processing more personal data than ever, and individuals are increasingly sharing their information online. As a result, data protection has become even more crucial. Both organisations and individuals must ensure that personal data is handled securely, responsibly and in compliance with legal requirements.

To promote awareness of data protection and privacy, the Division hosted an awareness-raising event at the Piazza. The event aimed to educate the public on their rights and responsibilities regarding personal data. Attendees received guidance, resources and practical advice on how to protect their information.

As part of this initiative, the Division encouraged members of the public to participate in a data protection survey which



assessed how much the public know about data protection; how aware they are about the use of their personal data; and which sectors individuals feel best protect their personal data. An online version of this survey was also made available on the GRA's social media platforms and a report highlighting the survey's key findings was published on Data Protection Day 2025. Further details on this topic will be provided later in the document.

The event was further strengthened by the support of the Gibraltar Youth Service, who joined to show their commitment to data protection awareness. Their participation reflected the importance of local collaboration and community engagement, reinforcing efforts to promote responsible data practices across all age groups.

To further amplify the reach of initiative, the event was covered on local news to help bring data protection issues to a wider audience. Media coverage plays a crucial role in raising public awareness, ensuring that key messages about privacy and security extend beyond the many who attended in person.

8 October 2024 – Presentation at the University of Gibraltar

The GRA's Director of Information Rights and Operations was invited to deliver a session on data protection and privacy to students of the MA in Leadership and Management and Master of Business Administration Courses.

As part of the module on New Technologies, the session highlighted the importance of data protection and privacy to individuals, society (including democracy and freedoms) and

business, particularly in the ever-growing use of digital technology both in business and public services. Referring to real life examples, the session highlighted the positive impact of new technology and risks to individuals, business and society – emphasising the importance and role of data protection as an enabler to protect individuals and promote innovation and success both in business (revenue generation and cost reduction) and public services.

This the third year in which the GRA has contributed to the University of Gibraltar's initiative to include data protection in its New Technologies module – embedding data protection and privacy into education is Privacy by Design at its finest.



25 February 2025 – Commonwealth Telecommunication Organisation (“CTO”) Digital Week Gibraltar: Action for Impact

The GRA's Director of Information Rights and Operations, presented at this event which brought together government leaders, regulators, industry pioneers and global stakeholders to discuss technological advancements and drive digital transformation across the Commonwealth.

In his presentation, the Director emphasised the importance of data governance in the public sector and referred to real-life examples to show that data protection and governance

is about protecting people, not just data. Four categories of harm were outlined with corresponding examples –

Annoyances, fear and psychological harm. A real-life scenario of a health practitioner accessing medical records without a valid reason was shown, where one of the victims said the breach left them worried and anxious, whilst another victim said the breach put them off going to see their doctor. The use of biased/inaccurate facial recognition technology by law enforcement and its aggravation of inequalities, referring to examples of wrongful arrests due to higher risks of misidentification in minority groups.

Financial costs. Reference was made to a case in the Netherlands where the Dutch tax authority wrongly accused an estimated 26,000 parents of making fraudulent childcare benefit claims, requiring them to pay back allowances they had received, driving families into severe financial hardship. Central to the problem was an automated system that perpetuated racial and ethnic bias. Reference was also made to the UK's Post Office Horizon scandal, in which nearly 1,000 individuals were wrongfully prosecuted for theft due to faulty data from the Horizon computer system. Some were imprisoned for false accounting and theft, while many others were financially ruined. As well as the cost to individuals, the costs to organisations was illustrated citing the UK NHS' near-£100 million costs of the WannaCry cyber-attack.

Physical harm. A BBC News investigation in the UK links IT system failures to the deaths of three patients and more than



one hundred instances of serious harm at NHS hospital trusts in England.

Death. The Director General of the World Health Organisation highlighted at a UN meeting that cyberattacks are not just issues of security and confidentiality; they can be issues of life and death. At best, these attacks cause disruption and financial loss. At worst, they undermine trust in the health systems on which people depend and even cause patient harm and death.

In addition to highlighting the role of data protection and governance in safeguarding individuals, organisations, and society, the session placed particular emphasis on their value as key enablers and drivers of innovation. The following points and examples were referenced in support –

Supporting Innovation – A GDPR objective. Alongside the protection of individuals another key (but sometimes overlooked) objective of the GDPR is to support economic growth, create new jobs and foster innovation – for example, as referenced in the European Commission's communications on the data protection reform that led to the GDPR (back in 2012).

Estonia. International media/reports widely recognise Estonia as one of the most advanced digital societies in the world.

Central to the success of “e-Estonia” is the “X-road”, which is a distributed information exchange platform that makes it possible for different systems to communicate across the governmental sector. Just from 5% of the queries managed via X-road, the platform is said to save approximately more than 820 years of working time for the state and its citizens annually. 95% of the savings are difficult to measure directly, as they occur automatically, but illustrates that the 820 years of working time gained is just the tip of the iceberg. The system has reduced the time taken to establish a business from 5 days to just 3 hours.

In its digital journey, Estonia states to have reached “unprecedented transparency” to build trust in its digital society, supported by a vision that, which has centred on the trust of citizens and where “personal data protection is the cornerstone of building trust towards e-Government”. Estonia emphasises that equally relevant to the opportunities created by technology is the importance of basic principles, such as transparency and privacy, considered fundamental to foster trust. Amongst Estonia’s e-government features is the “Data Tracker”, which allows citizens to always see who is accessing their data and for what

reasons.

The World Bank Group’s Identification for Development has recognised Estonia as a leading example as countries move to sustainable development towards the digital age, founded on key principles, which include Governance, trust, privacy and user rights.

Central Bank Digital Currencies. The recognition of the importance of data protection for innovation by key stakeholders other than DPAs, such as the Bank of International Settlements, the European Central Bank and the Bank of England in the context of Central Bank Digital Currencies. Project Tourbillon by the Bank of International Settlements concluded that privacy is a fundamental user requirement, citing a consultation from the European Central Bank where Privacy was identified as the feature that respondents wanted the most from the digital Euro. Also cited was a consultation from the Bank of England, which noted user privacy as one of the main concerns raised by respondents, recognising the critical importance of building the public’s trust in the digital pound and that privacy would be a “core design feature of the digital pound and an utmost priority”.

A Formula 1 analogy was used to explain how features like a strong braking system and regular pit stops (akin to data protection and governance) may seem to slow the car, but help it go faster and further while minimising risks - data protection and governance enable organisations to innovate, progress and protect individuals, society and themselves.

The GRA’s Director of Information Rights and Operations also joined a panel with Ms. Carina Kabajunga Wangwe (Chief Data Officer & Associate Director, UNICEF), Mr. Philip Victor (Partner and Managing Director, APAC, Welchman Keen) and Mr. Giovanni King (Chief Executive Officer Caribbean Datacentre Association).

Regulatory Matters

The following is an outline of the regulatory matters which the Division has been involved in for the period 2024/25.

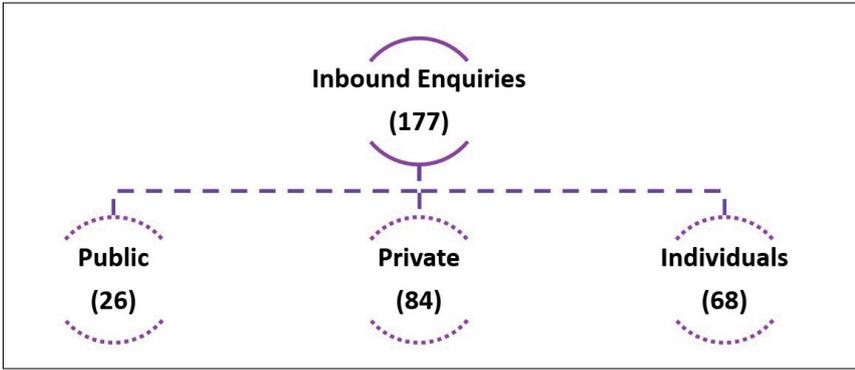
Measured Activity

The Division’s regulatory responsibilities include dealing with inbound enquiries, investigations, data protection audits, and data breach notifications.

Inbound Enquiries

The Division received 177 enquiries this year. Contrary to last year, half the overall tally received were enquiries from the private sector (84), followed by enquiries from individuals (68) and lastly by the public sector (26). This indicates that





businesses are actively seeking guidance on data protection compliance, while individuals are also engaging with privacy-related concerns.

The Division gathers insights into data protection issues affecting organisations and individuals in Gibraltar through various methods, with enquiries being a key source of information. By categorising these enquiries by subject, the Division can identify trends and adapt its work accordingly (e.g., organising specialised workshops and/or creating targeted guidance notes).

In comparison to last year, the number of inbound enquiries has increased by 8.5%. The month with the most inbound enquiries was July 2024 (22) and the least enquiries were received in December 2024 (9). Generally, enquiries fluctuated throughout the reporting period, with peaks in May 2024 and July 2024 for the public/private sector and individuals, respectively. This may indicate seasonal trends in compliance efforts or incidents prompting higher engagement with the Division.

For a fourth consecutive year, enquiries relating to subject access requests (“SARs”) (28) and CCTV (45) remain as the top 2 most popular topics, with enquiries relating to Breach Notifications trailing behind (14). The presence of varied topics suggests that organisations and individuals are seeking clarity on both regulatory compliance and rights under data protection laws.

Complaints, Investigations and Enforcement

An investigation involves the Division acting in response to a complaint or information obtained during its daily operations, where concerns arise about compliance with the Act and/or the Gibraltar GDPR. As part of its investigative role, the Division handles complaints from data subjects regarding data protection issues. The extent of each investigation varies based on the circumstances, with the level of involvement and resources required differing accordingly.

The Division encourages parties to resolve disputes amicably, following its complaint

procedure available on the GRA website. When this is not possible, further engagement may be necessary. This may lead to a formal Proposed Determination and Decision, which include remedial actions imposed by the Information Commissioner. In some cases, while formal action may not be required, extensive communication may still be needed to assess the issue and provide determinations, recommendations or guidance. This approach reflects the Division’s commitment to being a pragmatic and proportionate regulator while ensuring strong data protection measures for individuals.

A total of 51 new cases were opened during the period, while 48 cases were closed, showing a high-resolution rate and an efficient case-handling process. The majority of closed cases (40) were amicably resolved between the parties or were investigated typically through several rounds of lengthy communication, culminating in details recommendations to the relevant organisations but without the need for a concrete Proposed Determination and Decision. The reporting period saw the conclusion of 7 cases requiring this methodology, as detailed in the table opposite.

The investigations carried out during the reporting period for which Decisions were required are summarised in the table opposite, in order of date of closure:

| Cases | Q2 2024 | Q3 2024 | Q4 2024 | Q1 2025 | Total |
|--------------------------|---------|---------|---------|---------|-------|
| New | 11 | 20 | 8 | 12 | 51 |
| Closed | 12 | 10 | 12 | 14 | 48 |
| Active at end of quarter | 21 | 31 | 27 | 25 | |

| Reference Number, Data Controller, Date of Closure | Investigation Summary |
|--|--|
| C25/22 Royal Gibraltar Police (“RGP”) 1 October 2024 | This investigation concerned a response to a Subject Access Request. Articles breached: 12(4) and 15 of the Gibraltar GDPR. No further action was required, taking into account the circumstances of the case and corrective action taken. |
| C09/22 The Care Agency (the “Agency”) 3 October 2024 | This investigation concerned a response to a Subject Access Request as well as the redirecting of an email containing personal data. Articles breached: 5(1)(a) and 5(2) of the Gibraltar GDPR. No further action was required, taking into account the circumstances of the case and corrective action taken. |
| C17/22 RGP 15 November 2024 | This investigation concerned a response to a Subject access Request. Articles breached: 12(1), 12(2), 12(3), 12(5), and 15 of the Gibraltar GDPR Taking into account the circumstances of the investigation and corrective action taken by the RGP, the Information Commissioner closed this investigation. |
| C 22/21 Digital Services (“DS”) 18 November 2024 | This investigation concerned the information being provided to individuals within the e-gov portal’s (the “Portal”) privacy notice and cookie notice publicly available on HM Government of Gibraltar’s website, as well as cookie arrangements in respect of the Portal. DS is understood to be the data controller of the Portal. Articles breached: 6, 7(1), 7(3), 13(1)(a), 13(1)(b), 13(1)(c), 13(1)(f), 13(2)(a), 13(2)(b), 13(2)(c), 13(2)(d), 5(1)(a) and 12(1) of the Gibraltar GDPR. Regulations breached: 5(1) and 5(2) of the Privacy Regulations. Taking into account the circumstances of the investigation and corrective action taken by the DS, the Information Commissioner closed the case but reminded DS of its obligations to ensure compliance with the Privacy Regulations, the Gibraltar GDPR, and/or the Act. |
| C21/23 The Bike Club Limited (the “Club”) 21 November 2024 | This investigation concerned a complaint regarding the processing of the complainant’s personal data under Part III of the DPA for law enforcement purposes by the RGP, in relation to a renewal of a firearms licence. Articles breached: section 53, 54 and 61(6) of the Act. The RGP were required to ensure data subjects are provided with relevant information when applying for a firearms licence, they ensure adequate measures are in place to ensure RGP respond to SARs in a manner that complies with the DPA which facilitates data subject rights and that the RGP are able to demonstrate compliance with the above requirements. |
| C16/23 St Martins School (the “School”) 13 February 2025 | This investigation concerned the policies and procedures in place at the School aimed at protecting personal data pertaining to students, in particular relating to the photographs and recordings of students, from being deliberately or accidentally compromised. Articles breached: Article 5(1)(f), 5(2), 32(1)(d), 24(1) and 24(2) of the Gibraltar GDPR. The School were required to review their arrangements to ensure that appropriate policies and procedures were in place for the above-mentioned processing of personal data, taking into account that said processing may concern vulnerable students. The School were also required to demonstrate implementation of the same, and that relevant training would be provided to personnel as appropriate. Taking into account the circumstances of the investigation and corrective action taken by the School, the Information Commissioner closed the case but reminded the School of its obligations to ensure compliance with the Gibraltar GDPR and/or the Act. |
| C27/23 Mansion (Gibraltar) Limited (“Mansion”) 12 March 2025 | The investigation concerned Mansion’s alleged unlawful processing of personal data. Based on the information provided, no contravention of the Gibraltar GDPR and/or the Act was identified. |

Data Breach Notifications and Enforcement

Under data protection law, organisations must report certain incidents of non-compliance to the Information Commissioner. These are known as breach notifications and their reporting requirements are outlined in Article 33 of the Gibraltar GDPR (or section 76 of the Act for law enforcement processing).

Upon receiving a breach notification, the Division assesses the incident, reviewing the organisation's response and any ongoing privacy risks. Where necessary, further actions may be recommended to mitigate risks for affected individuals and prevent similar breaches in the future. In some cases, enforcement action may be taken.

During the reporting period, the Division handled 35 new data breach notifications in addition to several ongoing cases from the previous year. A total of 31 cases were closed, while 12 remain under investigation.

The most common types of breaches included cyber-attacks and unauthorised disclosures, together accounting for nearly half of all reported breaches. This indicates that both external and internal threats pose significant risks to data security. The Division has also seen an increase in the number of data breach notifications relating to insider threats which involves employees or internal actors

misusing their access to personal data. Whether intentional or due to negligence, insider threats can be difficult to detect and require strict access controls and monitoring to prevent misuse.

Data breaches were reported across various industries with the online gaming sector and financial services being the most affected. These industries typically handle large volumes of personal data, making them attractive targets for cybercriminals. Further, their reliance on digital platforms increases exposure to cyber threats, underscoring the need for strong encryption, fraud detection mechanisms and regulatory compliance to enhance security. The law enforcement sector also experienced multiple breaches this year, highlighting the risks associated with handling highly sensitive personal data. Breaches in this sector in particular, may compromise investigations or endanger individuals, making it crucial to implement strict security protocols and robust data handling procedures.

The Division emphasises the importance of ongoing engagement and regulatory cooperation in fostering a strong culture of data protection. Initiatives such as social media campaigns and workshops play a crucial role in educating and guiding DPOs. By equipping DPOs with the necessary knowledge and tools, these efforts empower them to raise awareness within

their organisations, ensuring that data protection remains a priority at all levels.

The breach notifications in respect of which enforcement action has been taken in the reporting year 2024/25, are summarised in the table opposite.

| BNs | Q2 2023 | Q3 2023 | Q4 2023 | Q1 2024 | Total |
|--------------------------|----------------|----------------|----------------|----------------|--------------|
| New | 4 | 7 | 13 | 7 | 31 |
| Closed | 6 | 10 | 10 | 9 | 35 |
| Active at end of quarter | 10 | 13 | 10 | 12 | |

| Reference Number Data Controller | Investigation Summary |
|--|---|
| BN19/23 Gibraltar Health Authority ("GHA") | The investigation concerned a data breach as submitted by the GHA on 9 October 2023, regarding the alleged unlawful disclosure of information by a former employee of the GHA. The Information Commissioner issued the GHA with an Information Notice on 9 February 2024. However, based on the information provided, no contravention of the Gibraltar GDPR and/or the Act was identified. |
| BN09/22 GHA | The investigation concerned a data breach as submitted by the GHA on 14 September 2022, regarding the unlawful disclosure of special category data (relating to 282 individuals) by a former employee to a legal representative. Articles breached: Article 5(1)(a), 5(1)(f), 5(2), 6(1), (9), 24(1), 24(2), 32, 34(1) and 34(2) of the Gibraltar GDPR. The Information Commissioner issued the GHA with a Reprimand on 12 November 2024. |
| BN04/23 Civil Status and Registration Office ("CSRO") | The investigation concerned a data breach as submitted by the CSRO on 23 June 2023, regarding the inappropriate accessing and subsequent disclosure of information. Articles breached: Article 5(1)(f), 5(2), 24(1), 24(2), 28(1), 28(3), 32, 34(1), 34(2) and 35 of the Gibraltar GDPR. The Information Commissioner issued the CSRO with a Reprimand on 18 December 2024. |

Data Protection Audits

Audits are conducted to ensure compliance with data protection laws and assist organisations in improving their data processing practices. While enforcement measures may be applied, when necessary, the primary objective of consensual audits is to provide guidance and support rather than impose administrative fines.

Although full-scale audits have not yet resumed, the Division has conducted in-depth reviews of various organisations' data protection practices. Through these exercises, the Division has provided guidance and recommendations to help organisations strengthen their compliance efforts. However, whilst the Division may offer guidance to support organisations in meeting their legal obligations, the Division does not approve or certify documentation. Organisations remain responsible for ensuring that their data processing activities comply with relevant legislation.

Data Protection Guidance

While the Division has not formally published specific guidance notes this year, the guidance provided to individuals and organisations has been delivered through the workshops held and by engaging directly with the relevant stakeholders. Providing clear and actionable guidance is a priority for the Division, and we remain committed to continuing this important work. Our ongoing efforts will focus on ensuring we are seen as an approachable regulatory, one that is always open to engagement and available to provide recommendations and guidance as required.

Registers

Register of DPOs

In accordance with section 138 of the Act, the Division continues to maintain a public Register of DPOs. To have a DPO listed in the register, organisations must complete and submit the DPO Notification Form that is available on the GRA's website.

The Opt-Out Register

The Division launched the Opt-Out Register for fax and telephone in 2013 in line with the provisions outlined in the Communications (Personal Data and Privacy) Regulations 2006. This regulation authorises the Division to oversee and maintain this Register. It is a free service that is available to fixed line and mobile subscribers who do not want to receive unsolicited direct marketing calls and/or faxes.

Public Awareness

The Division has continued its 'Control Your Privacy' campaign this year, to raise awareness of data protection and privacy matters.

a) Social Media

Social media plays a vital role in the Division's public engagement strategy. Through both ad hoc posts and larger campaigns, we share valuable privacy-related content with the public, often directing them to more in-depth resources such as infographics and guidance notes. All social

media campaigns are available in PDF format on the GRA's website.

This reporting year, the Division's social media activities have included the following:

DPO Social Media Campaign

This campaign aimed to raise awareness about the role of DPOs and the importance of their responsibilities in safeguarding personal data. The campaign was designed to complement the Information Commissioner's Guidance Note (3) IR03/17 which offers in-depth guidance on this topic.

Privacy Awareness School Report Social Media Campaign

This campaign featured key findings of the Division's Privacy Awareness School Report 2023-2024, which focused on the digital footprint. Its aim was to educate students, educators and parents on the importance of understanding and managing one's digital presence. By addressing the risks associated with digital footprints, the campaign promotes a greater awareness of privacy issues in the digital age.

A Privacy-Proof Countdown to Christmas

This social media campaign was launched during the festive season and featured 12 Christmas-themed privacy tips. The tips were shared on the GRA's social media platforms on each even day between the 2nd and 24th of December. The campaign was designed to be a timely reminder that data protection is an ongoing priority, even during the busy holiday season. The tips provided practical advice for individuals and organisations, reinforcing the idea that protecting personal data is a gift

that benefits everyone long after the holiday season ends.

Ad-hoc Social Media Posts

Throughout the reporting period, the Division has regularly utilised social media to deliver summarised data protection guidance to the public. Ad-hoc posts may vary from detailing activities carried out by the Division to providing guidance on certain topics that may be of interest. The posts may therefore cover topic areas such as the publishing of guidance notes, public and organisational awareness raising events, and participation in international events. For example, in the reporting year, there were individual posts on, amongst other things, international participation, the launch of the SME Resource Hub, local collaboration efforts, etc.

Audio Visuals

Constantly seeking ways to enhance and refresh its awareness-raising outreach strategies, the Division continues to create in-house audio-visual content. Through engaging, concise videos, the Division effectively shares guidance and simplifies complex concepts, making them more accessible and understandable. This year, the audio-visual content, available on both the GRA website and the Division's YouTube channel, has included the following:

Audio Visual: Key Definitions and the Legislative Framework

This audio-visual is part of the SME Resource Hub published by the Division and it provides a clear and engaging overview of key definitions within the legislative framework. It also highlights Gibraltar's data

protection landscape, including the changes introduced since Brexit. The video is visually engaging and informative, effectively simplifying complex legal concepts to make them more accessible to the target audience.

Audio Visual: Your Life, Your Data, Your Privacy

This audio visual was created to promote the Division's "Day in Town" event which took place in September.

Audio Visuals: Summer Top Tips

The Division re-published a video in which top tips are provided regarding the sharing of images online over the summer holidays.

Audio Visual: Ransomware

This audio-visual explores the growing prevalence of ransomware attacks, shedding light on what they are, how they work and the risks they pose. It forms part of the Gibraltar Regulator Forum's ongoing initiatives to help individuals and organisations better understand ransomware threats, recognise potential vulnerabilities and take proactive steps to mitigate risks.

Audio Visual: Data Protection, "Your Guiding Light"

This audio-visual is a festive, engaging reminder about the importance of safeguarding personal data during the Christmas season. Through catchy lyrics and cheerful music, the video highlights key steps for protecting privacy online, such as using strong passwords, avoiding phishing scams and ensuring the use of secure websites. It encourages viewers to take control of their digital presence, particularly during increasing online activity over the festive season.

Safer Internet Day

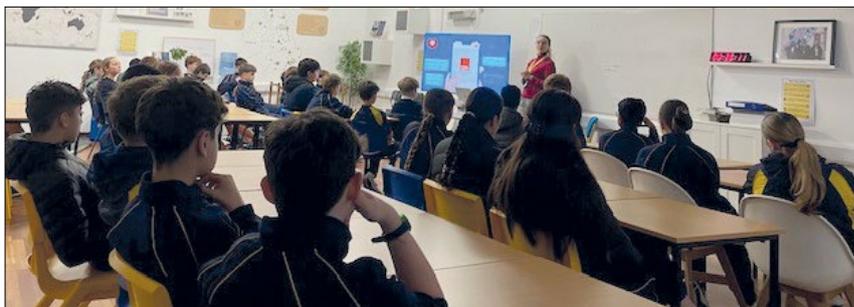
Safer Internet Day is observed every February to promote awareness of a safe internet for everyone, particularly for children and young people. This year, the Division marked the occasion with a social media post encouraging individuals to think carefully before sharing personal data online. The theme for this year, “Too Good To Be True”, focused on protecting yourself and others from online scams.

b) Awareness Through Education

Privacy Awareness School Presentations

Interactive presentations were delivered to students in Upper Primary and Secondary schools across the Year 5, 7 and 9 year groups with each presentation specifically tailored to suit the age and understanding of the target audience. While the content varied to reflect the development stage of each group, the core message remained the same: the importance of being aware of one’s digital footprint and the need to protect personal data, especially when using Social Networking Sites (“SNS”).

Throughout the presentations, students were educated on the significance of implementing appropriate privacy controls to maintain control over their digital presence. They are also made aware of the potential



risks of losing control over their privacy on SNS and the unintended consequences this could have.

Privacy Awareness School Report

Today’s digital environment can track online activity and build an intricate web of personal data particular to everyone. This web of information can include any data that is intentionally or unintentionally shared online through social media posts or likes, blogging profiles and online forms or, via data collected by third parties through cookies and tracking scripts. Data may also be collected through the sharing of photos and sending of emails; engaging in online debates and posting comments; internet browsing history; stored passwords; clicking on ads; subscriptions to newsletters; online purchases and reviews; the use of fitness trackers etc.

As has been the case in previous years, the Division published a report and infographic that relates to the results of a survey carried out in schools in Gibraltar between October and April of

the 2023/24 academic year (the “Survey”). The Survey specifically focused on the students’ awareness and understanding of their digital footprints, affording them an opportunity to properly consider their digital presence and the impact of their online interactions.

The Survey forms part of an ongoing awareness-raising initiative organised by the GRA in-cooperation with HM Government of Gibraltar’s Department of Education. A total of 1332 students between the ages of 9 and 14 years completed the Survey and key findings, as outlined in the report, are summarised below –

800 students believed their digital footprint started as a result of their parents/guardians posting photos/videos of them, as a baby/child.

Only 5% of students said they did not use the internet or online sites/apps.

90% of the students stated that they were aged 12 and under when they started contributing to their digital footprint.

The most common platform to share personal data on was WhatsApp.

78%, 67% and 53% of the Year 9s, 7s and 5s, respectively, recognised personal data shared can remain online forever.

The Division remains steadfast in that broadening the scope for privacy awareness is imperative, in particular to promote the secure and appropriate use of SNS amongst students. The Information Commissioner recognises that completely erasing a digital footprint may be difficult/impossible, however, there are ways for individuals to better take control over their digital presence and reap the benefits of online sources

without compromising privacy and security (e.g., limiting the personal data disclosed, regulating privacy settings, implementing strong passwords, etc). These adjustments can mitigate potential threats and protect individuals from identity theft, privacy invasion, and social engineering attacks.

The Information Commissioner will continue to monitor students' habits in future initiatives and, where appropriate, may extend these initiatives to the wider population to further the understanding of data protection and privacy-related matters in today's ever-increasing online environment.

The full report is available to download from the GRA's website.

awareness of the importance of privacy and data protection, particularly in light of the ever-increasing challenges faced in our increasingly globalised and digitised world.

To celebrate Data Protection Day this year, the Division published a report on the results of a Data Protection Survey (the "DP Survey") launched in September 2024 and which aimed to assess public awareness about data protection. The results of the DP Survey help determine whether the data protection issues prioritised by the Information Commissioner, based on inbound complaints and enquiries, align with the concerns of the community or, if additional issues in other areas require attention. This insight will shape the Division's forward action plan and identify areas to focus on.

In the following, some of the Survey's key findings are outlined:

61% of respondents felt some level of control over their personal data, a decline from 83% in comparison to the results identified in its first survey carried out in January 2020 (the "First Survey"), potentially attributed to the introduction of an additional option "it depends on the organisation," chosen by 21% in the DP Survey.

Respondents were most concerned about data shared through mobile phone applications and least concerned about store or loyalty card data, though around 40% expressed general concern about all processing activities.

Majority of respondents disagree that providing personal information is a minor issue or acceptable in exchange for free services, echoing findings from

PRIVACY AWARENESS SCHOOL SURVEY 2023-24

YOUR DIGITAL FOOTPRINT

Illustrated below are the key findings from the Privacy Awareness School Survey (the "Survey") carried out in schools in Gibraltar between October 2023 and April 2024. This year, the Survey specifically focused on the students' awareness and understanding of their digital footprint.

The Survey consisted of six multiple-choice questions and was made available to all students between the ages of 9 and 14 years either in paper format or using an online platform, as based on the schools' preference.

The start of your digital footprint

Students were asked whether their digital footprint began even before they started using the internet. **200 students** followed their digital footprint started as a result of their parents/guardians posting photos/videos of them, as a baby/child in the online environment.

1332 students undertook the survey.

44% Year 5 students (aged 9-10 years)
35% Year 7 students (aged 11-12 years)
63% Year 9 students (aged 13-14 years)

Illustration A: Did your parents/guardians post photos/videos of you online, as a baby/child?

| Year | Yes | No | Don't know |
|--------|------|------|------------|
| Year 5 | ~100 | ~100 | ~100 |
| Year 7 | ~150 | ~100 | ~100 |
| Year 9 | ~250 | ~100 | ~100 |

Adding to your digital footprint

Only 5% of students said they did not use the internet or online sites/apps. Of the remaining 95% of students, approximately 90% stated that they were asked to post photos/videos when they started contributing to their digital footprint through their use of the internet and/or online sites/apps.

Online sites/apps used by the students, or the content they are being exposed to on the internet, may not be age appropriate. The age restrictions in place ensure minimum ages 13 years so younger children are likely (and inadvertently) compromising their privacy and/or exposing their personal data when engaging in the online environment.

INSTALLING/DOWNLOADING APPS

Users will likely be asked to grant permission for personal data (e.g. contacts, location, camera) to be accessed by the app provider/platform for the app to work as intended. However, there may be instances where the personal data is shared with third parties for alternative purposes (e.g. direct marketing), which the students may not be fully aware of.

c) E-Newsletters

E-newsletters continue to be released periodically, offering subscribers information, updates, and the latest news regarding data protection and freedom of information as relate to Gibraltar and the Division's work. Prepared in-house, the Division's e-newsletters are circulated amongst subscribers and are also accessible on the GRA's website.

d) Subscription Service

The Division offers a subscription service for people and groups wanting updates on data protection issues. This service includes updates on ongoing work, such as the release of Guidance Notes and new content on the GRA website. Those wishing to subscribe can do so on the GRA website.

e) Data Protection Day

Data Protection Day is an annual event celebrated internationally on 28 January. Its aim is to raise

Students access to online accounts that require a password

Year 5 & Year 7 students (42% and 53% respectively) managed an online account which an adult they trusted created for them.

64% of Year 9 students typically gained access to an app by creating their own online account.

23% of Year 6 students accessed the online environment by using a parent/guardian's account and login credentials.

Sharing personal data in an online environment

The most common platform used to share personal data was WhatsApp with 63% of students stating they shared personal data in WhatsApp groups comprised only of people they knew.

Sharing personal data via private chat functions in apps like Snapchat, TikTok and Instagram was also popular amongst 45% of students.

Before sharing information online, about yourself or others, ask yourself: Who will see this post? Is there anything in this post that gives away sensitive information? Is sharing this information necessary?

If you don't know or don't like the answer to any of these questions, reconsider whether to share it.

The effects of sharing personal data online

In today's digital era, sharing personal moments and connecting with others has become increasingly effortless. However, it is crucial to be aware of the risks that come with oversharing personal data online. The personal data shared online can sometimes remain online forever. This was recognised by 78%, 67% and 53% of the Year 9, Year 7 and Year 5 students, respectively.

Deleting a digital footprint is an almost impossible task, given that an individual's online activity has traces of linked information, which may be stored in places unbeknownst to them (e.g., third-party services, search engines, social media platforms, Government databases, etc.).

PRIVACY SETTINGS

Take control over your digital presence & reap the benefits of the online environment without compromising privacy & security by **limiting** the personal data you disclose, **regulating** privacy settings, be cautious of accepting requests from unknown accounts and by **implementing strong passwords**.

DOWNLOAD THE FULL REPORT FROM OUR WEBSITE
<https://www.gra.gi/data-protection/privacy-awareness/school-campaign>

the First Survey.

88% of respondents are very concerned about organisations using their information for undisclosed purposes, an increase from 75% in the First Survey.

When assessing whether respondents were appropriately briefed by organisations in relation to the processing of their personal data, the private sector was rated more favourably, indicating greater proactivity and/or consistency in communication by private organisations.

Results revealed varied trust levels, including heightened concerns about data privacy in digital and tech sectors in comparison to private banks and medical services.

87% of respondents are aware of the GRA's role in enforcing data protection laws, reflecting successful outreach efforts which will continue to be further developed.

As the data protection landscape continues to evolve, it remains critical for both organisations and individuals to adapt to emerging challenges and ensure the responsible management of personal information. The Information Commissioner plays a vital role in this process. His continued efforts are essential in fostering a well-informed approach to privacy and ensuring all stakeholders are equipped to understand and appropriately navigate the evolving regulatory environment.

The full report is available to download from the GRA's website.

Freedom of Information ("FOI")

Gibraltar's Freedom of Information Act 2018 is founded on the principle that individuals have a right to access information about the activities of public authorities, unless there is a valid reason to withhold it.

Understanding the importance of FOI and access, the Division remains actively involved, where appropriate, in international discussions and correspondence on topics related to FOI.

Professional Development initiatives

The Division is committed to fostering a knowledgeable and skilled workforce to effectively carry out its regulatory duties. To support this, it consistently seeks opportunities to improve and enhance professional development, viewing it as a valuable investment in its staff.

Internal training sessions, organised by the Division, for the Division, have provided valuable opportunities for both presenters and participants to enhance their skills – whether by gaining confidence in delivering the presentations, improving the visual quality of training materials or deepening their understanding of new topics.



Broadcasting



Introduction

The responsibilities of the Broadcasting Division (the “Division”), as set out in the Broadcasting Act 2012 (the “Act”), are to:

- Grant licenses to broadcasters;
- Enforce the conditions set on licensees;
- Regulate matters on broadcasting standards;
- Issuing codes of practice; and
- Encourage the promotion of media literacy.

The Division specialises in providing guidance to consumers, purchasers, and other users of the broadcasting services in Gibraltar, including the public service broadcaster with whom the Division maintains a good working relationship.

There are five media service providers that fall under the jurisdiction of Gibraltar. These are:

1. The Gibraltar Broadcasting Corporation (“GBC”). GBC is the sole media service provider with a public service remit. GBC provides a television broadcasting service and a radio broadcasting service, Radio Gibraltar;
2. The British Forces Broadcasting Service, provided by the Services Sound and Vision Corporation, is a radio broadcasting service;
3. Music Box Gibraltar, is an audiovisual media service that offers international and local music videos 24/7 and transmits via the cable networks;
4. The Gibraltar Football Association (“GFA TV”) is an

audiovisual media service that offers local and international football matches, as well as sport news, and transmits via the cable networks; and

5. Gibfibre VOD, is a subscription-based video-on-demand service that offers adult content to Gibfibre customers only.

International Participation

59th meeting of the European Platform for Regulatory Authorities (“EPRA”), Rotterdam, 5th to 7th June 2024

The 59th meeting of EPRA took place in Rotterdam, the Netherlands, from 5th to 7th June 2024. A total of 137 participants from 51 regulatory authorities attended the meeting.

The first plenary session focused on media literacy and elections. In a year that was marked by geopolitical instability, policymakers at both national and European levels placed increasing expectations on media literacy as a key lever

for safeguarding information integrity, particularly in the context of elections. The discussion centred on ways that improved media literacy would help to counter disinformation but also strengthening democratic resilience and fostering greater civic participation.

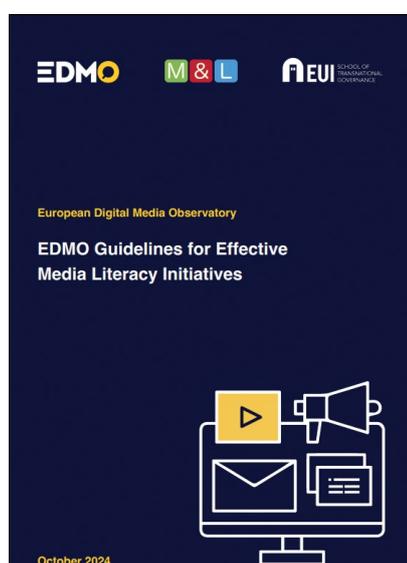
The second plenary session focused on the increasing integration of artificial intelligence (“AI”) across the media sector, and how this was significantly reshaping both existing business models and the regulatory frameworks that have evolved over decades to support them. This transformation risked deepening the disparity between large audiovisual players who possess the resources to leverage their data and invest in cutting-edge infrastructure, and smaller, often more vulnerable media outlets. At the same time, AI will accelerate the entry of powerful new actors into the media ecosystem.

For media regulators, such as the GRA, staying ahead of this technological evolution is essential. Building a deep, operational understanding of AI will be critical to maintaining relevance, credibility, and influence in shaping future media policy.



GRA Endorsement of the European Digital Media Observatory (“EDMO”) Guidelines for Effective Media Literacy Initiatives, 16th October 2024

The GRA endorsed the guidelines, developed by the EDMO Council on Effective Media Literacy Initiatives, which consist of 12 key principles. These principles will help to support media literacy initiatives from development to implementation and evaluation. They will also play a vital role in fostering critical thinking skills and helping people navigate today's complex media landscape. These guidelines will help create media literacy initiatives to counter misinformation and help promote informed and responsible engagement across digital and traditional media platforms.



60th meeting of EPRA, Limassol, 23rd to 25th October 2024

The 60th EPRA meeting was held in Limassol, Cyprus, from 23rd to 25th October 2024. Over 128 participants from over 45 member countries also attended the meeting.

The first plenary session focused on the impact of AI on media and the implications for media regulators. The discussion centred on the motivation for the use of AI in the media industry with the main reasons being automation, simplification and scaling. The use of AI makes it possible to expand to areas without detailed knowledge and years of experience. AI tools make it possible to create artistic images quickly and without detailed knowledge with a few content specifications.

For media regulators, this raises numerous challenges. The discussion highlighted issues such as ownership of AI created content and determining where the responsibilities lie. With the further development of AI technology, the detection of deepfakes will also become increasingly difficult which can lead to a general loss of trust in the media. The issue of transparency will become an even greater challenge with the increasing mixing of traditional media content with AI-generated content.



The following is an outline of the regulatory matters which the Division has been involved with during the reporting period 2024/2025.

Measured Activity

Inbound Enquiries

The Division continues to receive queries on matters relating to the GRA's codes of practice, as well as dealing with queries about applications for television and radio licences.

Monitoring

The Division continues to have a good working relationship with local broadcasters and is always available to provide guidance and make recommendations. The Division systematically monitors and logs broadcasting content to ensure that media service providers are complying with all the relevant codes of practice.

Throughout this reporting year, 93 programmes that were broadcast by GBC were recorded and monitored for compliance. The content of the programmes were varied and covered different genres i.e. news, current affairs, community, and magazine. The GRA is pleased to note that all the programmes recorded were compliant with all the relevant codes of practice.

Complaints

The GRA received no formal complaints during this reporting year.

Administrative Notice with respect to Complaints made against the Gibraltar Broadcasting Corporation in relation to broadcasting matters

On 10th May 2024, an Administrative Notice was issued in accordance with section 13(1) of the Act, setting out the GRA's remit in relation to complaints made under section 62 of the

Act against GBC in relation to its discretionary powers with respect to broadcasting content.

Public Consultation - Code on due impartiality, due accuracy and undue prominence

On 29th May 2024, the GRA began a consultation process on proposed amendments to the Code on due impartiality, due accuracy and undue prominence (the "Code"). The GRA asked the views of all interested parties for their views in relation to:

1. "Composition of panels", referring to the assembling of panels for a debate on Controversial Matters or Policy Matters, (pages 16-17 of the Code);
2. "Political broadcasts not made in relation to any election or referendum", (pages 23-24 of the Code); and
3. "Political broadcasts made in relation to an election or referendum" (pages 26-27 of the Code).

Although the purpose of the consultation was to allow all relevant stakeholders to make representations to the proposed amendments above, it also provided them with an opportunity to make representations to the GRA of any additional concerns, comments or suggestions as regards any aspects of the Code.

As a result of the feedback received, the GRA made revisions to its first consultation, and published an additional consultation on 24th February 2025 that was edited to reflect the concerns noted in responses to its first consultation.

Once the GRA has completed its review of the Code and made

further amendments based on issues raised by all stakeholders, the GRA will publish the names of the respondents and their responses on its website. The GRA envisages this to take place later in the year.

'Media Literacy Matters' Campaign

The GRA has a duty, under the Communications Act 2006, to promote media literacy and better public awareness and understanding of any material published on electronic media. The responsibilities assigned to the GRA commenced on 27th July 2023 and allows for a better public understanding of the associated risks of electronic media content, and how material is selected and made available for publication via electronic media.

The Division, having launched its 'Media Literacy Matters' Campaign (the "Campaign") on 6th November 2023, has continued to expand on this and is engaging with the community. The GRA recognises the significance of communicating with stakeholders as it facilitates outreach to the wider community to help promote media literacy. To date, the GRA has reached out to the following organisations:

- Gibraltar Youth Centre
- GibSams
- Childline Gibraltar
- Clubhouse Gibraltar
- PossAbilities Gibraltar
- Royal Gibraltar Police
- Gibraltar Senior Citizens

Media Literacy Partnership Programme

The Division initiated the creation of a media literacy partnership with organisations which would favourably benefit from being media literacy ambassadors in Gibraltar. All the organisations mentioned above have all shown a keen interest and welcomed the initiative.

The GRA believes this partnership will make a lasting impact on the educational landscape in Gibraltar and shape the future of digital engagement. Ambassadors will be able to empower individuals to navigate the digital age with confidence, fostering critical thinking, responsible digital citizenship, and informed media consumption among our community.

GBC – The Powder Room Interview

On 16th July 2024, a member of the Division appeared on the "Powder Room" in order to promote the GRA's Media Literacy Campaign and generate a greater public understanding of the potential for online harm, fake news and misinformation as a result of material published on electronic media.

The interview, which featured a panel, discussed the GRA's revised duties under the Communications Act 2006 to promote media literacy. Additionally, the following matters were also discussed:

- General overview of media literacy
- Dangers of online harm
- GRA - Media Literacy Survey
- Artificial Intelligence and Deepfakes
- GRA's Powers and Regulatory Remit

GBC – Summer Camp Participation

For the second year running, the Division was invited to attend a session as part of GBC's Summer Camp. GBC's Summer Camp for children aged between 10 to 14, is a two week programme designed to teach them the skills to write, direct, film and produce their own stories and content.

On 24th July 2024, two members of the Division, as part of its media literacy campaign, were invited to present an interactive session on the dangers of fake news, especially on social media platforms, as well as the growing trend of influencers targeting young users on the most popular social media platforms. The feedback received from the GBC CEO was very positive, and the children thoroughly enjoyed the interaction presentation.

EPRA - Media Literacy and Information Working Group

The Division has played an active role in EPRA's Media and Information Literacy Working Group ("EMIL"), a dynamic forum dedicated to advancing media literacy across Europe. Participation in EMIL has not only reinforced our strategic engagement at a European level but has also allowed the Division to share an insight regarding the development of its own Media Literacy Matters campaign. Over the course of the reporting year, the Division contributed to three EMIL meetings, strengthening collaboration and knowledge exchange with fellow regulators and media literacy stakeholders.

EPRA - Artificial Intelligence and Regulators Roundtable

The AI Roundtables consists of a closed group of EPRA members willing to share and learn on all things AI and regulation-related, and notably on the use and development of AI-based tools by and for regulators.

Although the GRA does not at present use any AI-based tools for the regulation of broadcasting content, the GRA is nevertheless keen to learn about the use of AI-based tools by regulators. The roundtable sessions provide an insight into the opportunities and challenges presented by these AI tools, and the Division has participated in two meetings in this reporting year.

Media Audiovisual Visualisation Information System Europe ("MAVISE") Workshop on Free Ad-supported Television ("FAST")

The GRA is included in the MAVISE database, a free access database that provides information on the audiovisual media services and video sharing platforms available in Greater Europe. The database is managed by the European Audiovisual Observatory ("EAO") and is updated monthly, allowing interactive searches of the registries of the European audiovisual regulatory authorities.

The EAO organised an online workshop for regulators on the challenges of regulating FAST channels, given its rapid growth. The discussions focused on the blurring lines between traditional broadcasting and on-demand platforms. The main concerns raised were questions regarding jurisdiction as many operate cross-border making it difficult for regulators to

enforce compliance; advertising and transparency as many FAST providers are not subject to consistent content and advertising standards thereby raising concerns about content targeting minors.

xi. Revenue Collected

During the period 2024/2025, and in accordance with the provisions of the Broadcasting (Licensing) Regulations 2019, the GRA collected a total of £13,000 in respect of the following Licences:

| | |
|-----------------------------------|---------|
| FM Radio Licence | £10,000 |
| Audiovisual Media Service Licence | £3,000 |



Postal Services



Introduction

The Postal Services Division (the “Division”) of the GRA is responsible for the granting and enforcement of licences and general authorisations issued to postal service providers. In addition to this, the Division has the responsibility of regulating the postal sector in Gibraltar in accordance with the provisions of the Post Office Act 1961 (the “Act”) and the Postal Services (Authorisation) Regulations 2012 (the “Regulations”).

Specific functions under the Act, include monitoring the operational developments of the Royal Gibraltar Post Office (the “RGPO”) as the designated Universal Service Provider (the “USP”) setting quality standards, monitoring performance against these standards and ensuring that the RGPO complies with its universal service obligations which ultimately secures the provision of an efficient universal postal service at an affordable price for all users in Gibraltar. This must be achieved whilst balancing the RGPO’s right and freedom to also provide competitive services in a fully liberalised postal market.

The Division also has a responsibility to ensure that the RGPO complies with its obligations arising from the Act, as well as any additional regulatory measures imposed by the GRA relating to the provision of universal service. In many instances, this includes issuing guidance and directions in respect of accounting procedures, best practice and quality standards to improve the myriad of services currently available to consumers in Gibraltar.

The GRA also issues general guidance and recommendations to all postal service providers to ensure compliance with the requirements of the Act and that the rights of users are upheld, especially in cases where complaints are not satisfactorily resolved.

Regulatory Matters

The following is an outline of the regulatory matters carried out by the Division for the period 2024/25.

Universal Service

The universal service obligation aims to ensure that every user has the right to a universal service involving the permanent provision of a postal service of specified quality at all points in Gibraltar at affordable prices.

The GRA designated the RGPO as the USP until 6th August 2027. It is important to note that whilst the RGPO’s individual licence safeguards the provision of universal services and ensures compliance with essential requirements, it is in fact the RGPO’s designation which imposes the various universal service obligations. As the designated USP, the RGPO must provide a minimum range of services of a specified standard and affordable price for all users in Gibraltar.

The specific universal service obligations referred to above relate to the following:

- Quality of postal services;
- Affordability of postal services;
- Density of points of contact

and access points;

- One clearance and one delivery to the home of every natural or legal person or appropriate installation;
- The clearance, sorting, transport, and distribution of postal items up to 2 kgs;
- The clearance, sorting, transport, and distribution of postal packages up to 20 kgs;
- Provision of services for registered and insured items;
- Provision of certain free services for blind and partially sighted persons;
- Redirection and return to sender services;
- Poste Restante;
- PO Box;
- Local and cross-border Mail.

The RGPO is also responsible for the delivery of incoming international mail to addresses within Gibraltar and collection and onward transmission of outgoing international mail. Among other items, the RGPO’s individual licence ensures that the universal services listed above evolve to meet the needs of consumers and that they are made available without any form of discrimination and are not interrupted. The individual licence also ensures that a suitable level of information is made available to consumers in respect of universal services and that complaints handling procedures are fair and conducted in a timely manner.

Essential Requirements

In accordance with the Act, the GRA may impose what are described as “essential requirements” on the supply of postal services in Gibraltar. These requirements shall be based on the following non-economic reasons –

- a) the confidentiality of correspondence; and
- b) the security of the network as regards the transport of dangerous goods.

The GRA published Notice No. P03/2020 which imposed a number of revised essential requirements on all postal service providers in Gibraltar and not solely upon the RGPO. The GRA also revoked the previous essential requirements that were applicable at the time, ultimately ensuring that all postal service providers in Gibraltar establish and apply adequate procedures that may be deemed necessary for the purpose of minimising the exposure of postal items to the risk of loss, theft, damage, or interference and for the management of access and prevention of unauthorised access to mail.

The “essential requirements” also enforced an obligation on all postal service providers to keep their procedures under regular review to ensure that these matters are adequate and that the confidentiality of any correspondence or general mail sent is ultimately maintained. In order to assist all local postal service providers, the Division regularly publishes guidance in relation to “protecting the integrity of mail” which includes information on best practice to assist local postal service providers in establishing the necessary mail integrity procedures that are, among other things, suitable for their own individual needs and size of their network and workforce.

The GRA is also of the view that each individual postal service provider should have the freedom and flexibility to tailor their own procedures and policies to their own

circumstances when it comes to maintaining the confidentiality of correspondence. The main areas covered in the GRA’s guidelines and whereby operators may exercise an element of flexibility in terms of the standards imposed are:

- Recruitment;
- Disciplinary Procedures;
- Agents and Sub-contractors;
- Security of mail; and
- Information and Reporting Requirements.

Quality of Service Requirements - Local Mail

In accordance with the provisions of Section 40 (1) of the Act, the GRA has a duty to set quality standards for local mail by considering and striking a balance between Gibraltar’s unique topographical and geographical circumstances and how this would relate to any given postal service provider insofar as it related to the collection, sorting and subsequent delivery of mail. In doing so, the GRA, upon consultation with the RGPO, often establishes this delivery standard and reviews this periodically in order to ensure the provision of a good quality universal postal service.

The quality-of-service target for local mail is expressed according to the formula (D+N) where D represents the date of deposit (before the last collection time of the day) and N is the number of days which elapse between that date and the delivery to the addressee.

The standard for the next day delivery of local mail has been set as follows:

- 95% of items to be delivered in Gibraltar the day after posting (D+1).



Performance Monitoring - Gibraltar Public Services Ombudsman

Section 4N(4) of the Act requires independent performance monitoring of the established quality standards to be carried out. To date, this task has been carried out successfully by the Gibraltar Public Services Ombudsman (the “GPSO”) who, with the approval of the GRA, has acted as the independent body tasked with monitoring quality of service targets for local mail throughout Gibraltar.

The GPSO are currently monitoring the full local end-to-end network, which involves the collection of mail from various access points and subsequent processing and delivery within Gibraltar. The GPSO fulfils this

task by sending out numerous test letters to a broad spectrum of members of the public who then report receipt of these letters. This ensures that the full local end-to-end network, which involves the collection of mail locally from various access points and subsequent processing and delivery within Gibraltar, is monitored.

With the above in mind, it is vital to note that the RGPO has previously raised concerns over the accuracy and reliability of the performance statistics provided, due to the potential for error, which it believes are inherent in the current monitoring system. In response to this the Division advised the RGPO to meet with the GPSO in order to tackle this directly by revising the manual procedures currently in place.

The GPSO and RGPO have since been exploring the viability of incorporating the use of automated systems that would enhance the overall accuracy of all performance results moving forward.

The Division often uses the statistical data collected to assist the RGPO in making informed decisions on its operations, as well as conceiving and implementing operational improvements that are ultimately designed to assist them in meeting the established quality of service standards.

International Inbound Delivery within Gibraltar

As the USP for Gibraltar, the RGPO has a duty to monitor its quality of service and in addition to the mail monitoring by the GPSO, the RGPO has also been part of the Global Monitoring System (the "GMS") since 2011. This is an independent performance measurement system managed

by the Universal Postal Union (the "UPU"). The UPU coordinates postal policies among member nations and aims to streamline the global network with a view to maintaining adequate postal services and finding ways to improve quality of service for customers. Gibraltar is a member of the UPU as an overseas territory of the United Kingdom.

The GMS consists of external, independent panellists who exchange test items between the participating countries. The test items contain a radio frequency identification "RFID" tag which is read by an antenna installed at the RGPO sorting office where the international mail is received and processed. The test items are identified and logged automatically and once delivered, this information is immediately sent to the UPU to determine the quality of service being provided. This information is used to determine remuneration between postal administrations, according to their performance standards. In other words, the performance results generated by the GMS are linked to the setting of terminal dues payments. This in turn determines the payment rates in mail exchanges between countries and subsequently affects remuneration between postal operators, based on their performance.

However, it is important not to confuse this system which only monitors the processing and delivery times of inbound international mail once it arrives in the sorting office, which is then processed and delivered with that of the GPSO which monitors the full local end-to-end network which entails the collection of mail from access points, processing and delivery within Gibraltar. In other words, it is in essence a "last-mile"

measurement rather than a full "end-to-end" measurement.

The local delivery target established by the UPU for this purpose is 88% (D+1).

Access Points

In accordance with the provisions of section 4A of the Act, the GRA has a duty to ensure that every user has the right to a universal service involving the permanent provision of a postal service of specified quality at all points in Gibraltar. The GRA shall, to this end, ensure that the density of the points of contact and of the access points takes account the needs of users. In this regard an access point essentially means physical facilities, including letter boxes and/or pillar boxes which are provided for the public either on the public highway or at the premises of the postal service provider in question, in this case the RGPO.

Complaints and Dispute Resolution

All postal service providers in Gibraltar are required to have procedures in place for dealing with complaints and handling disputes. In the first instance, customers are required to contact their postal service provider with their complaint and allow them adequate time to investigate and resolve any issues.

Where a complaint has not been satisfactorily resolved, the customer may then file a complaint with the GRA. However, the GRA can only consider genuine and reasonable complaints regarding postal services offered in Gibraltar by authorised service providers.

In accordance with the provisions of Section 4P(8) of the Act, the RGPO, as the designated USP, is required to publish information on the number of complaints received and the manner in which they have been dealt with.

Internet Revolution and Liberalisation of the Postal Sector

The internet revolution has transformed the economics of postal services around the world. It will come as no surprise that the internet has reduced the demand for letter mail because emails are a generally free and quicker alternative means of communication, thereby reducing revenue collected for letter mail significantly. Conversely, it has boosted the demand for parcel mail as online shopping has taken a growing share of the retail market, potentially to the detriment of the high street retail stores.

The designated USP, in Gibraltar's case the RGPO, has no choice but to rise to meet these challenges posed by the current state of the postal market both locally and internationally. From a regulatory perspective, the RGPO has made significant operational changes in order to meet the requirements of the fast-growing market for parcels. In addition to this, the liberalisation of the market has also had a huge impact due to the fact that alternative operators are able to provide similar services at more competitive prices and in some instances have the option or freedom to "cherry pick" the most lucrative products and destinations as dictated by customer demand. The designated USP is not afforded this luxury and is instead required to provide a world-wide service

regardless of attractiveness from a revenue standpoint. As a result, designated USP's have been under pressure to find ways of reducing the cost of providing universal service.

With the above in mind this huge shift in the postal services sector is something that the GRA as well as other regulatory bodies around the world are aware of and must take due account of, if and when regulatory intervention is needed.

Social Media

The Division uses social media platforms to ensure that consumers are provided up to date information or appropriate guidance where applicable, on numerous topics of interest which are relevant at the time and relate to postal services.

The Division has previously published information and guidance, by way of social media slides on the following topics:

- Sale of stamps & pricing;
- Addressing properly;
- Articles for the Blind;
- Redirection of Mail;
- Access Point locations and changes;
- Changes to opening times throughout the year; and
- Latest recommended posting dates for Christmas etc.

The Register

The Regulations require the GRA to establish and maintain a register of authorised persons and individual licences granted by the GRA under Part I of the Act.

The Register can be inspected at the GRA's office and is also accessible on the GRA's website.

Revenue Collected

During the 2024/2025 period and in accordance with the provisions of the Act, the total amount collected by the GRA in respect of General Authorisations was £1,000. The total amount collected by the GRA in respect of the Individual Licences issued to the RGPO was £5,000. This has brought the total revenue for Individual Licences and General Authorisations for 2024/2025 period to £6,000.



Higher Education Regulation



Introduction

On 31st May 2018, the University of Gibraltar (Regulation and Accountability) Regulations 2018 (the "Regulations") were commenced and the GRA was designated as both the Gibraltar Higher Education Commission, and the Gibraltar Authority for Standards in Higher Education.

The Higher Education Regulation Division (the "Division") was setup by the GRA in accordance with Part 11 of the University of Gibraltar Act 2015 (the "Act") and specifically to perform the roles of both the Gibraltar Higher Education Commission, and the Gibraltar Authority for Standards in Higher Education.

Regulatory Matters

Role and responsibilities of the Higher Education Regulation Division

The Act requires the Gibraltar Authority for Standards in Higher Education to:-

- establish criteria for the recognition of qualifications awarded by the University Of Gibraltar (the "University");
- keep and maintain a register of the University's qualifications; and
- promote the quality and standards of university education and training through a system of quality assurance of courses, academic programmes, and awards.

The GRA also acts as the Gibraltar Higher Education Commission, which is tasked with monitoring compliance with the University's duties and obligations under the Act. On 1st June 2018, the GRA issued a Memorandum of Regulation ("MoR") to the University. Since then, the MoR has formed the cornerstone of its regulatory framework. On 1st November 2022, a revised MoR was developed in consultation with the University and it set out how the GRA:-

- Monitors the quality and standards of education in the University;
- Monitors compliance by the University with its functions, duties and obligations under the University of Gibraltar Act 2015 ("the Act");
- Monitors the use by the University of its funds including any public funds provided to it;
- Monitors other aspects of the University performance;
- Expects the University to demonstrate effective governance and accountability;
- Expects the University's autonomy and academic freedom to be maintained.

Memorandum of Regulation

The original MoR set out the process by which the University would provide annual documentation to support their developments and improvements in all aspects including governance, facilities, quality of courses and financial sustainability. The revised MoR recognised the achievements of the University to date and provides more detail on the annual documentation and assurances the University must continue to provide.

As part of its responsibilities,

the Division continues to carry out a desktop analysis of the documentation and assurances provided by the University.

The Division has agreed to meet with the University, in early April, to discuss the results of the desktop analysis and the annual risk assessment. The Division has also scheduled to meet regularly for updates on the University's progress through the next academic year. Overall, the Division liaises closely with the University and maintains a good working relationship.

Graduations

The University held its graduation ceremony on 7th December 2024, during which 78 students received their awards after successfully completing their studies. The ceremony was held for the third time at the Europa Point Sports Complex in order to accommodate all the graduates, families and guests.

The following is a breakdown of the number of graduates per course:

| Courses | Graduates |
|--|-----------|
| Bachelor of Business Administration (Hons) | 8 |
| BSc Adult Nursing | 16 |
| BSc Maritime Science Nautical | 5 |
| BSc Maritime Science Eng | 3 |
| Master of Business Administration (MBA) | 1 |
| MA Leadership and Management | 3 |
| Postgraduate Certificate in Education (PGCE) | 19 |
| MSc Marine Science and Climate Change | 13 |
| Environmental Science and Climate Change | 2 |
| MSc Clinical Psychology | 6 |
| PhD | 2 |

The Vice Chancellor addressed the 78 graduates by congratulating them and stating how proud all the University team were of their achievements. She outlined how the University ensured all its programmes were industry relevant and of the highest quality, and how, for every graduating cohort to date, this had supported an employment rate of between 92 to 97% within 6 months of graduating. She also added that, according to a recent survey, 96% of Gibraltar University students felt satisfied that the knowledge and skills they took away from their programme would support their career aspirations.

The University's Chancellor, Sir Lindsay Hoyle, spoke to the graduating students, about the hard work and resilience needed to complete their studies saying - "You are a credit to the University, to Gibraltar and to yourselves, and I would like to wish you all the very best of luck. Take the experiences that you have gained and use them to inform new ones. Take the knowledge that you have attained and use it to transform your life and the lives of those around you. Today is your day, but it is also your tomorrow".



Quality Assurance

The Regulations and the MoR require the University to undergo a quality review, and this was successfully completed on 14th March 2022. The International Quality Review (IQR) was conducted by the Quality Assurance Agency for Higher Education (QAA).

The QAA is the independent expert quality body for higher education across the UK and the IRQ offers institutions outside the UK the opportunity to have a review benchmarked against international quality assurance standards.

The successful IRQ review means that the University is fully accredited by the QAA, and they can use and display the IQR Accreditation Badge on their website and marketing material as a mark of excellence.

In September 2024, a visiting QAA team conducted a Scheduled Mid-Cycle Review on-site and in November 2024, the University retained its Global Accreditation by the QAA following the successful outcome of the Review. The next QAA review is expected to take place in 2026, before the end of the current five-year accreditation cycle ending in January 2027.



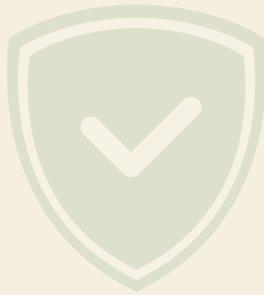
University of Gibraltar Higher Education Courses 2024 -2025

Undergraduate

Bachelor of Business Administration (Hons)
 BSc (Hons) Computing and Entrepreneurship
 BSc (Hons) Adult Nursing (we also have students on the Diploma in Adult Nursing which is a variation of the BSc (Hons) Adult Nursing Programme)
 BSc (Hons) Maritime Science (Engineering) with Engineer Cadetship Programme
 BSc (Hons) Maritime Science (Nautical) with Deck Cadetship programme

Postgraduate

MA Leadership and Management
 Masters of Business Administration
 Masters of Business Administration (Gaming)
 Postgraduate Certificate in Education
 Masters in Education (MEd.)
 MSc in Marine Science and Climate Change
 MSc in Environmental Science and Climate Change
 MSc Contemporary Healthcare
 PhD



Cyber Security Compliance



Introduction

The Network and Information Systems (NIS) Directive (EU 2016/1148) was the first cybersecurity law to cover the whole of the European Union (EU) and was intended to improve the overall cybersecurity level for critical infrastructure in the EU. This Directive was transposed to Gibraltar legislation in 2018, as Part 7 of the Civil Contingencies Act 2007 (the "Act").

On 16th January 2023 the NIS 2 Directive (EU) 2022/2555, entered into force for Member States, broadening its coverage with more sectors being required to enhance their cybersecurity measures. It standardises the reporting obligations and establishes a structure for handling cyber crises. All Member States were required to transpose the NIS 2 Directive into their national legislative frameworks by 17th October 2024.

The UK is no longer a member of the EU and is not required to implement the NIS 2 Directive, however, following a consultation in 2022 the UK government proposed to expand the range of digital service providers (DSPs) to managed service providers (MSPs) and a market study on MSPs was carried out. The GRA is closely monitoring any changes to the UK NIS regulation and to international legislation on cybersecurity.

The Role of the Competent Authority

Under Part 7 of the Act, the GRA is designated as the competent authority for the security of network and information systems in respect of operators

of essential services (OESs) and DSPs. The GRA's Cyber Security Compliance Division (the "Division") responsibilities are as follows:

- Regulating, supervising and enforcing compliance with the Act;
- Establishing a list of operators of essential services;
- Establishing a list of digital service providers;
- Investigating breaches;
- Issuing guidance to OESs or DSPs;
- Drawing up Codes of Practice;
- Recording and reporting incident notifications; and
- Conducting or organising inspections.

The GRA is also designated as the single point of contact (the "SPOC") for Gibraltar, under section 38(4) of the Act. The SPOC's role largely concerns cross-border co-operation where cyber incidents affect multiple countries and exchange of information is required.

International Participation

CYBERUK Conference 2024

The UK Government's flagship cyber security event took place in May 2024 in Birmingham. The National Cyber Security Centre (the "NCSC") organised

the conference with the focus on "Future Tech, Future Threat, Future Ready". CYBERUK 2024 examined how future technology represents significant opportunity, from employing AI in pioneering healthcare research, to using quantum computers to solve problems like climate change and food security. However, to harness the benefits, the cyber security sector must ensure that new and developing technologies are secure by design and, vulnerabilities are mitigated. The conference successfully served as a platform for sharing insights and best practices across the whole industry.

Three GRA members of staff attended the conference and in between the presentations, masterclasses and workshops, they were able to meet some of the other regulators and exhibitors.

UK Cyber Regulators' Forum

The Division regularly attends the Cyber Regulators' Forum (the "Forum") organised by the NCSC. These meetings allow for the oversight bodies and regulators of the different NIS sectors to discuss lessons learnt and to share industry specific nuances and threats that have been identified.

On 24th September 2024 and 28th January 2025 respectively, the GRA participated in the Forums, hosted online, which covered topics such as incident management, quantum computing effects and the cyber



skills framework.

On 26th November 2024, two representatives from the GRA attended the Forum hosted in London, where speakers from the NCSC, the Office for Nuclear Regulation (ONR) and the Information Commissioner's Office (ICO) gave updates on their various regulatory approaches to cybersecurity. Following the Forum, the NCSC provided a presentation on the Cyber Assessment Framework (the "CAF") which allowed a deep dive into the changes proposed for version 4.

Further to the work being carried out by the Forum, additional working groups have been created to address specific issues. The GRA participates in the Cyber Resilience Audit Working Group which is developing a new industry assurance scheme in which UK commercial providers are being encouraged to get accredited to carry out cyber resilience assessments on behalf of the oversight bodies and regulators.

UK Overseas Territories Cyber Security Community Building Conference

The Head of Division attended on 3rd-7th February 2025, the 4th annual UK Overseas Territories Cyber Security Community Building Conference hosted in Gibraltar by the UK Government and HMGoG. The conference

focused on building strong working relationships among the UK Overseas Territories and creating a platform for sharing experience and knowledge.

The week's agenda included sessions on:

- Cyber Security Governance.
- Implementing Necessary Security Protections.
- Conducting a National Cyber Risk Assessment (NCRA).
- Establishing Cyber-Attack Detection Capabilities.
- Effective and Rapid Incident Response.

The conference combined both presentations and hands-on exercises to assist with cyber incident identification and mitigation.

Regulatory Matters

The following is an outline of the regulatory matters which the Division has been working on during the reporting year.

Report on Designation of Operators of Essential Services

The GRA is responsible for designating operators of essential services insofar as their network and information systems are essential for the

maintenance of critical societal or economic activities in Gibraltar.

The Act requires the GRA to assess the following sectors:

- Energy
- Transport
- Banking (pending derogation)
- Financial Market Infrastructures (pending derogation)
- Health Sector
- Drinking Water Supply and Distribution
- Digital Infrastructure

In March 2024, the Division commenced a review of the Health Sector and contacted a wide range of providers of health care services in Gibraltar, including hospitals, general health clinics, pharmacies, mental health service providers and dental clinics among others. On completion of the review, the Division identified and designated an additional OES in the health sector.

Designation of Digital Service Providers

Providers of digital services such as online marketplaces, online search engines or cloud computing service are identified as DSPs under the Act and just like OESs, they must ensure the level of security of their systems are appropriate to the risks identified and as far as possible minimise the impact of any cyber incident. DSPs must also notify the GRA of any incident which has a significant impact on the provision of their digital services.

Reporting of Incidents

The OESs and DSPs are required under sections 42(1) and 43(3) of the Act respectively, to notify the Division of any incident that may



have a substantial impact on the provision of the essential service.

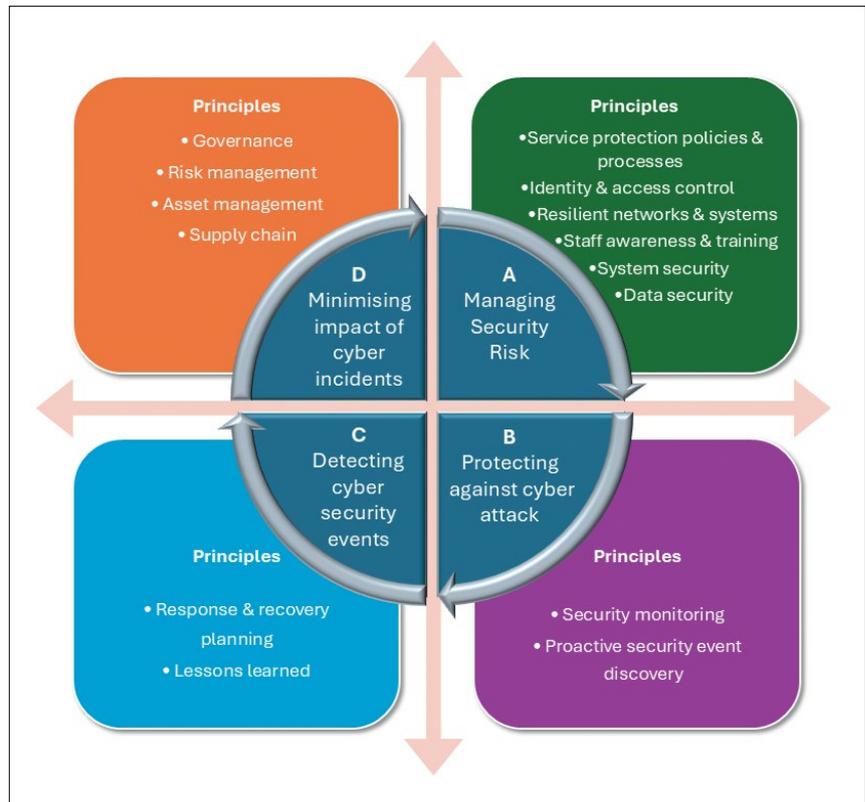
The reporting of incidents is done via the NIS reporting form available on the GRA's website and should be submitted as soon as possible but no later than 72 hours after becoming aware of the incident.

Voluntary Reporting of Incidents

A separate online voluntary reporting form is also available on the GRA's website. Any organisation may notify the GRA of cyber incidents that may have impacted on the continuity of their services. It must be stressed that the GRA will not provide direct feedback on how to resolve or mitigate the effects of a cyber incident but encourages organisations to submit any information they feel is appropriate. All incident information received will be collated and will be included with intelligence from other sources and used to update the cybersecurity threat landscape for Gibraltar. This in turn will assist in developing appropriate guidance and alerts.

Assessment Framework

The Act requires OESs to take appropriate and proportionate technical and organisational measures to manage the risks to the security of network and information systems which support the delivery of essential services. The CAF guides OESs through fourteen NIS cyber security principles which have been written in terms of outcomes. The CAF is primarily an assessment tool that specifies what needs to be achieved rather than what needs to be done. The



Division is currently looking at implementing CAF version 4 by the end of the year.

The CAF is based on four main objectives and structured into specific principles that are based on sets of indicators of good practice. For further information on the assessment process and the CAF, please visit the Cyber Security Compliance section on the GRA's website.

Inspections

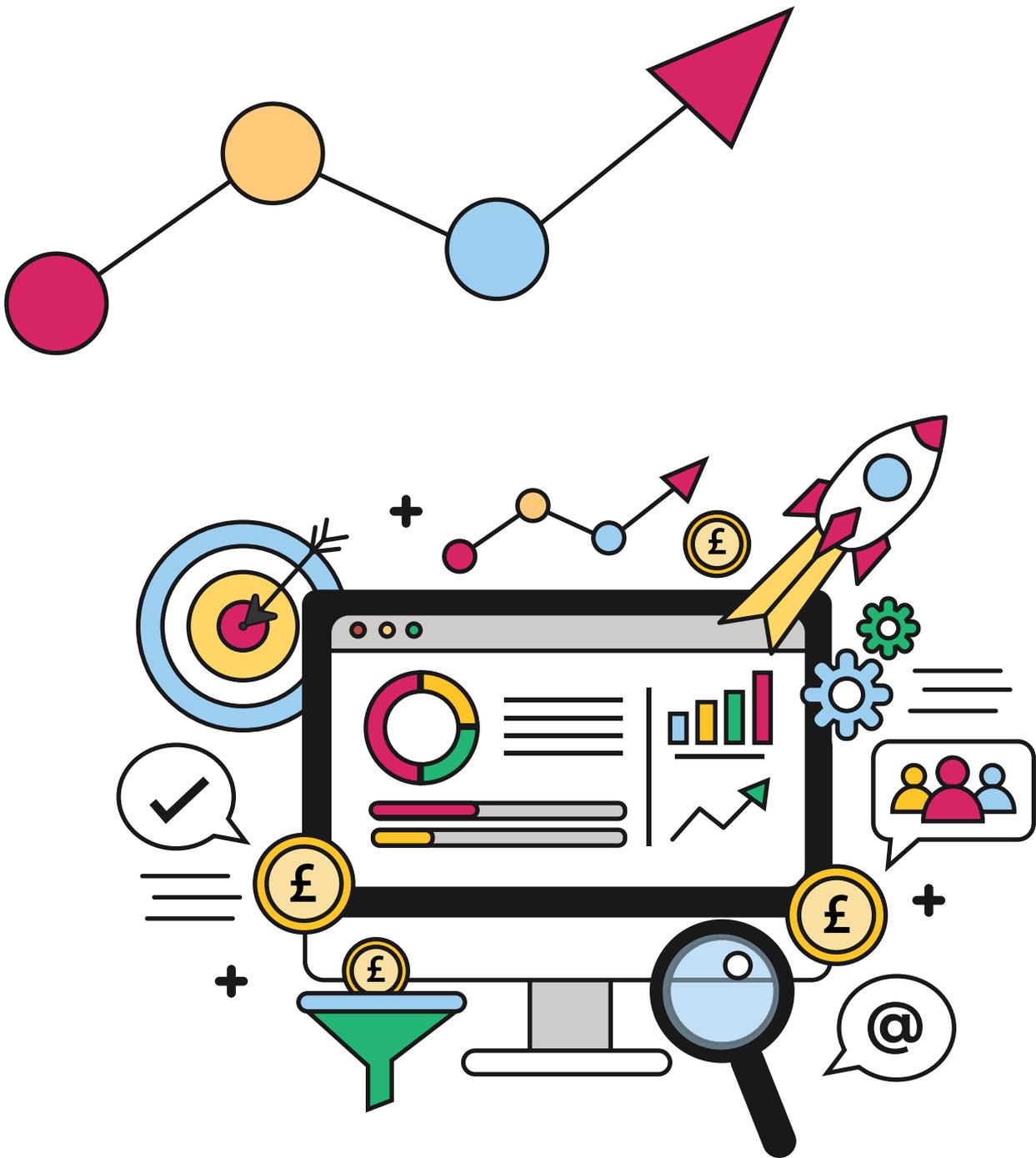
Several inspections on specific areas were carried out during 2024 and recommendations were made to improve cybersecurity. The inspections will continue in 2025 to address resilience and service continuity in greater depth.

Liaison with other Bodies

The Division is liaising with the designated OESs to identify the possible cyber security risks that need to be addressed

in each sector. As part of the GRA's requirements and in accordance with sections 38 and 40 of the Act, the Division is cooperating closely with the Gibraltar Computer Security Incident Response Team and with Gibraltar law enforcement authorities. Internationally, as the designated SPOC, the Division continues to liaise with the UK's Government Communications Headquarters and NCSC.

Competition



Introduction

The Gibraltar Regulatory Authority (the “GRA”) is designated as the competent authority for the promotion and enforcement of competition law in Gibraltar. Pursuant to such designation, the GRA must discharge all the functions, duties and obligations in accordance with the Competition Act 2020 (the “Act”), acting in its capacity as the Gibraltar Competition and Markets Authority (the “GCMA”).

The mission of the GCMA is to make markets work well in the interests of consumers, businesses, and the economy. Competition provides firms with incentives to deliver what consumers want, provide value for money, produce efficiently and innovate. Thus, well-informed, active consumers can play a key role in driving competition between businesses.

The GCMA aims to work with Government, other regulators, industry and the public to oversee certain business transactions and enforce competition rules. Its mandate includes assessing agreements between firms, regulating abuses of a dominant position, conducting market studies and market investigations, reviewing mergers, dealing with specific types of complaints, and investigating cartels. The GCMA also has the function of publishing guidance on all competition matters, making proposals and providing advice to Government Ministers and making the public aware of ways in which competition may benefit consumers and the economy of Gibraltar.

In line with its public awareness

duties under the Act, the GCMA continues its main focus of preparing and publishing guidance material and its policy statements on a whole range of competition law issues. The GCMA is ready to respond to queries and aid businesses and the general public on any area of the law. It is also branching out into the international sphere by contacting other similar sized competition regulators in order to learn from their experiences, exchange ideas and discuss pressing matters which affect us all.

International Participation

Advanced EU Competition Law – 26th to 27th November 2024

One member of the GCMA attended an advanced EU competition law conference in Brussels in order to gain further insight into the competition cases currently being dealt with by national regulators in Europe.

Day one of the conference highlighted discussions on competition policies,

investigations and enforcement. The workshops and breakout sessions concentrated on the recent sports cases, cartels and leniency, lessons learnt from private enforcement and legal professional privilege considerations. Exchanges were provided by the European Commission, competition regulators from Italy, Belgium, Austria and Germany together with industry professionals representing large firms such as Carlsberg, Audi and Nokia.

A judge’s roundtable on how cases are handled initiated day two of the conference followed by presentations on merger control, market definition, digital markets, abuse of dominance and dawn raids and compliance. Legal firm representatives and competition consultants provided the main content and feedback for the day’s sessions with smaller individual workshops also being available on specific matters affecting different markets across Europe. The conference also provided an opportunity to meet other colleagues and network with other regulators in an effort to exchange information and facilitate any cross jurisdictional investigations.



Regulatory Matters

In accordance with the Act, the GCMA has a duty to provide public awareness on the ways in which competition may benefit consumers and the economy of Gibraltar. Issuing information and advice to the relevant Government Minister or any public authority, also forms part of its role. Furthermore, the GCMA has a legal obligation to prepare and publish guidance material and statements of policy (the "Guidelines") on its responsibilities and use of its powers regarding agreements between undertakings, the assessment of dominance, mergers, and market investigations amongst others. Before publication or revision of the Guidelines, the GCMA is required to consult with any such persons it considers appropriate. These persons may include, but are not limited to, other regulatory authorities, legal practitioners, business associations, individual businesses and their customers, and the public.

Public Consultation and Decision Notice

On 22nd January 2024, the GCMA launched public consultation CP02/24 regarding a series of guidelines and policy statements (the "Guidelines") in relation to the Chapter 1 Prohibition (agreements between undertakings), the Chapter 2 Prohibition (abuse of dominance), mergers and market investigations.

The seven Guidelines consisted of:

1. The Chapter 1 Prohibition;

The Chapter 1 prohibition (section 3 of the Act) concerns agreements between undertakings, decisions by associations of undertakings or concerted practices ("agreements") which may affect trade within Gibraltar and have as their object or effect the prevention, restriction, or distortion of competition within Gibraltar.

2. The Chapter 2 Prohibition;

The Chapter 2 prohibition (section 10 of the Act) explains that any conduct on the part of one or more undertakings which amounts to the abuse of a dominant position in a market is prohibited if it may affect trade within Gibraltar.

3. Merger Assessment Guidelines;

This document provides advice and information about the making and consideration of merger references under section 74 (completed mergers) and 85 (anticipated mergers) of the Act and the way in which relevant customer benefits may affect the taking of enforcement action by the GCMA.

4. Merger Remedies Notice;

The Merger Remedies Notice specifies the information and documents to be submitted by the merger parties for the purpose of offering undertakings in lieu of reference ("UIL"), pursuant to section 128 of the Act.

5. Market Investigation References;

Under section 191 of the Act, the GCMA may make a market investigation reference to its Chair for the constitution of a group where it has reasonable

grounds for suspecting that any feature, or combination of features, of a market in Gibraltar for goods or services prevents, restricts, or distorts competition in connection with the supply or acquisition of any goods or services in Gibraltar.

6. Merger and Market Remedies – Reporting, Investigation and Enforcement of potential breaches;

This policy statement covers the GCMA's approach to actual or potential breaches of final undertakings and orders put in place to address concerns identified in merger and market investigations under the Act; and

7. Merger and Market Remedies – Variation and Termination of Merger and Market final undertakings and orders.

This policy statement covers the GCMA's approach to the variation and termination of merger and market final undertakings and orders.

The GCMA invited all interested parties to provide comments on the questions set out in the public consultation and the closing date for submission of comments was Friday 29th March 2024. The GCMA received comments from GibFibre Ltd, an electronic communications firm and the Gibraltar Association of Compliance Officers (GACO). After taking these into account, the GCMA published Decision Notice C09/24 on the Chapter 1 and Chapter 2 prohibitions, mergers and market investigations together with the final version of the Guidelines mentioned above. The decision notice and the Guidelines can be found on the competition section of the GRA's website.

Public Consultation and Decision

In line with its publication and awareness duties, on 16th January 2025 the GCMA conducted a consultation on another series of guidelines and policy statements regarding its investigation procedures, mergers, cartels and penalties.

Public Consultation CP01/25 dealt with the following documents:

Investigation Procedures

This guidance document provides general information for the business and legal communities and other interested parties on the processes that the GCMA uses when using its powers under the Act to investigate suspected infringements of competition law. The Act prohibits, in certain circumstances, agreements, decisions and concerted practices which prevent, restrict or distort competition (the Chapter 1 prohibition) and conduct which constitutes an abuse of a dominant position (the Chapter 2 prohibition).

Interim measures in merger cases

This policy statement has been issued under section 153(1) of the Act which stipulates that the GCMA must prepare and publish a statement of policy in relation to the use of its powers under section 151, insofar as they relate to interim measures, and section 152. This policy is intended for merging parties and for legal representatives advising on a transaction where interim measures may be relevant.

Applications for leniency in cartel cases

This guidance sets out the detail of how the GCMA will

handle applications for leniency for civil investigations into infringements by undertakings (the Chapter 1 Prohibition) and immunity from prosecution for criminal investigations into cartel offences by individuals. The GCMA's leniency policy enhances and facilitates its enforcement actions against cartel conduct.

Cartel prosecutions

This guidance is issued under section 266(1) of the Act, which stipulates that the GCMA must prepare and publish guidance on the principles to be applied in determining, in any case, whether proceedings for a criminal cartel offence under the Act should be instituted.

Administrative penalties

This document sets out the GCMA's statement of policy regarding its powers under section 42 of the Act to impose penalties on a person who fails to comply with a requirement imposed under:

Section 14 – Investigations: powers to require documents and information;

Section 15 – Investigations: power to ask questions;

Section 16 – Power to enter business premises without a warrant;

Section 17 – Power to enter business premises under a warrant;

Section 18 – Power to enter domestic premises under a warrant;

Section 41 – Information relating to transferred EU anti-trust commitments and transferred EU anti-trust directions.

The GCMA invited all interested parties to provide comments on the questions set out in the public consultation and the closing date

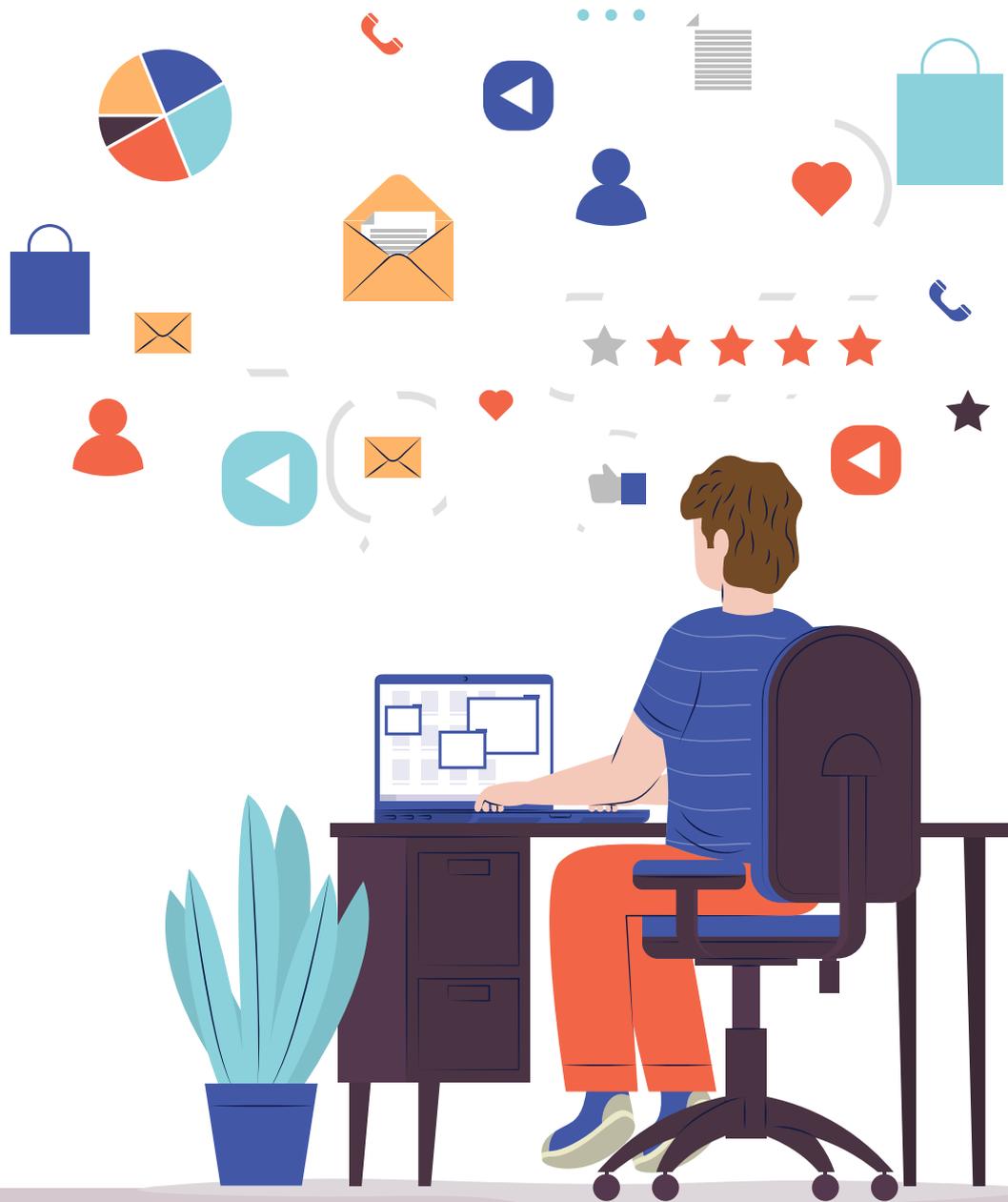
for submission of comments was Friday 28th February 2025. The GCMA took the utmost account of all comments received and published Decision Notice C02/25 on its investigation procedures, mergers, cartels and penalties together with the final version of the guidelines and policy statements mentioned above. The decision notice and the guidelines can be found on the competition section of the GRA's website.

Networking

The GCMA has been reaching out to other national competition authorities in order to establish a network where information can be shared in an open and confidential way. Learning from other regulators' experience is vital to improve outcomes where the GCMA reviews mergers, investigates cartels or simply provides guidance and advice to industry and consumers alike.

The Competition and Markets Authority in the UK has wide ranging knowledge of how markets work well and what action needs to be taken to improve conditions for businesses. Additionally, the GCMA has approached the competition regulators from Jersey and Guernsey given their similarities in terms of resources and size and has also commenced talks with the Irish Competition and Consumer Protection Commission on how information can be exchanged regarding tailor made solutions for specific problems to ensure the best results possible. The GCMA will be reaching out to other regulators during the course of the year in an effort to expand its network and acquire knowledge in this new field of regulation.

Accessibility



Introduction

The Accessibility Compliance Division (the "Division") was setup to assess compliance of Public Sector Bodies ("PSB") in accordance with the Public Sector Bodies (Websites and Mobile Applications) Accessibility Regulations 2018 (the "Regulations"). A PSB refers to HMGoG, bodies governed by public law, or associations formed by one or more bodies governed by public law, if those associations are established for the specific purpose of meeting needs in the general interest, not having an industrial or commercial character. Bodies governed by public law are bodies that are established for the specific purpose of meeting needs in the general interest, do not have an industrial or commercial character, possess legal personality, and they have any of the following characteristics:

1. they are financed, for the most part, by Government or by other bodies governed by public law;
2. they are subject to management supervision by Government or those other bodies;
3. they have an administrative, managerial or supervisory board, more than half of whose members are appointed by

Government or by other bodies governed by public law.

The relevant PSBs must endeavour to offer their websites and mobile applications in a format which is perceivable, operable, understandable and robust, so that all members of society, including those with disabilities, are able to partake in the functions of those PSBs. PSB are not required to comply if doing so would impose a disproportionate burden on that PSB, although in order to assess this, an assessment must be carried out, explain its findings of that assessment and aim to provide alternatives if they are unable to comply.

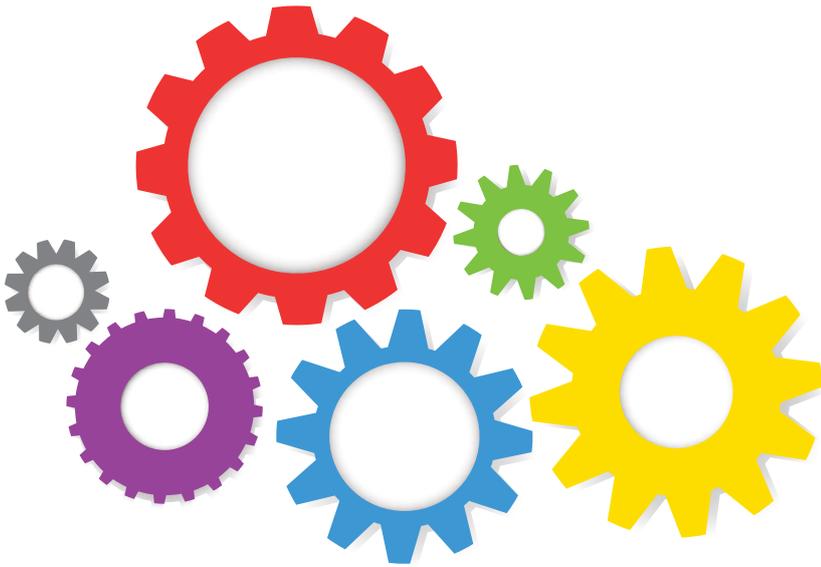
The Division is tasked with monitoring compliance with the requirements of the Regulations and must ensure that PSBs put in place mechanisms with which to receive notifications from persons who believe that the relevant website or mobile application has failed to comply. Furthermore, the Division is responsible for receiving complaints from those persons who believe that responses from the affected PSB has not been satisfactory. To this end, the Division has developed an electronic Complaints form and published this on the Accessibility Compliance section of the GRA website.

The Division has made efforts to identify those PSBs which may be captured by the Regulations and is currently in the process of liaising with HMGoG so that the various websites under the ownership of Government Departments, take steps to meet the requirements of the Regulations. The Division is also working closely with its own Information Systems team to take those same steps with its own website. The Division is in the process of developing guidance for PSBs on how to make their websites accessible.



GRA

**GIBRALTAR REGULATORY
AUTHORITY**



**2nd Floor,
Eurotowers 4,
1 Europort Road,
Gibraltar**

Tel: 200 74636



www.gra.gi