REPORT ON THE RESULTS DERIVED FROM THE DATA PROTECTION SURVEY

INTRODUCTION

For organisations, protecting the personal data of individuals is an issue of risk and trust. On the one hand, protecting personal data mitigates the likelihood of significant, costly incidents, including reputational loss and regulatory penalties. On the other hand, protecting personal data is also essential to an individual's trust in the organisation. Organisations depend upon the trust of their existing and prospective customers, clients, business partners, vendors, and employees. When this trust is lost, it can have a devastating impact on both the organisation and the individual.

The Gibraltar Regulatory Authority (the "GRA"), as Information Commissioner (the "Commissioner"), carried out a public Data Protection Survey (the "Survey") to learn about the public's -

a. awareness of data protection;
b. awareness in respect of the use of their personal data; and,
c. trust in how personal data is being handled by public and private sector service providers.

PURPOSE AND METHODOLOGY

The Survey consisted of 17 questions, predominantly Likert-scale questions. The purpose of the Survey was to learn about the public's awareness of data protection and their perception in regard to the importance of privacy and data protection and the work of the Commissioner's office. The results help identify whether the data protection areas focussed on by the Commissioner's office as a result of inbound complaints and/or enquiries, are consistent with concerns within our community, or whether there are additional concerns in other areas. This information will help guide and inform the Commissioner's action plan on areas that his office should look to focus on.

Published in October 2019, the Survey was made available on the GRA's social media platforms, including Facebook, Twitter and LinkedIn for a period of 3 months.

A total 120 responses were received.

SURVEY RESULTS

The Commissioner believes that public awareness about data protection has increased in recent years. The Commissioner's belief is supported by the continuous increase in the number of data protection complaints and inbound enquiries received by his office over the past few years. As a result of greater data protection awareness, the public are more aware of their rights over their data and are better able to identify data protection issues.

Demographics

In terms of gender, out of the 120 responses received, 48% of these pertained to the male population and 52% pertained to the female population.

In terms of age demographic, the pie chart below shows that approximately half of the total number of responses received related to individuals ranging between 31 and 45 years of age.

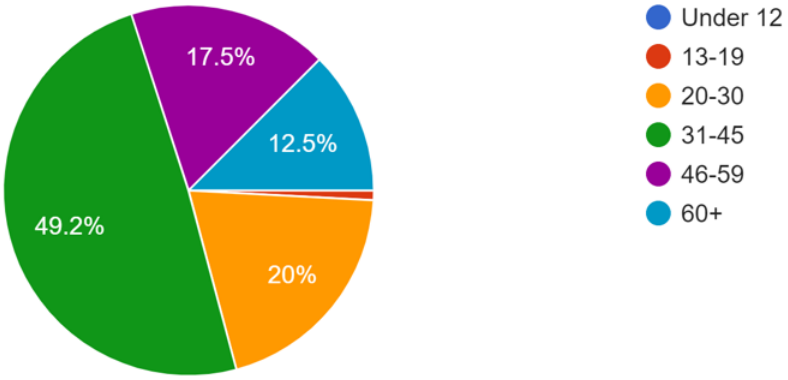


Illustration A - Age demographics

The Commissioner's office's conclusions from the Survey are summarised in the following.

1. How much control do you feel you have over the information you provide to organisations?

In the Survey, respondents were asked to rate how much control they felt they had over the information provided to organisations (e.g. the ability to correct, change or delete this information) by classifying their assessment into three categories: complete control, partial control or no control at all.

Results show that over 74% categorised their 'level of control' as "partial control" with only around 9% stating that they felt they had "complete control" over the information provided to organisations.

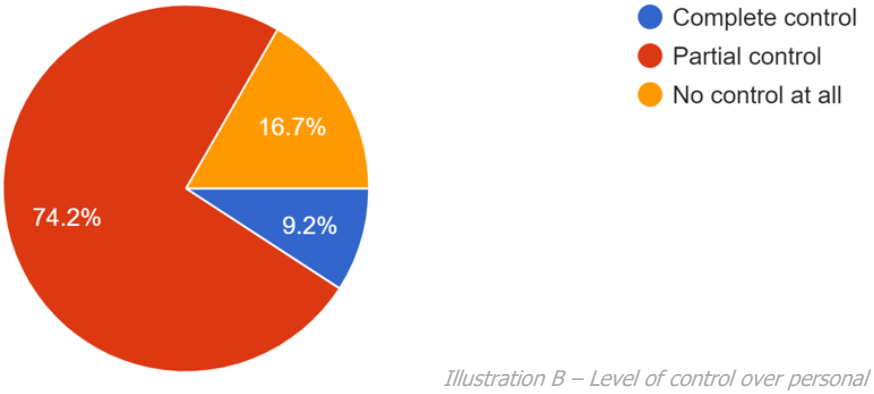


Illustration B – Level of control over personal data provided to organisations

This result is concerning given the introduction of the EU General Data Protection Regulation 2016/679 (the "GDPR") and its emphasis on enhancing the rights and control of individuals over their personal data.

When processing personal data, organisations are required to provide individuals with clear, concise information relating to the rights of the respective individuals and the use(s) of their personal data, including information such as for what purposes the data will be used for, the legal basis for processing of that data, and with whom the data will be shared. These are just a few of the requirements listed under Article 13 of the GDPR relating to the information that must be provided to an individual at the point of data collection.

The Commissioner is of the view that the more individuals are informed about the processing of their personal data and their rights, the greater control they'll have in terms of exercising their data protection rights.

In view of the above, the Commissioner aims to investigate local organisations to identify whether individuals are being provided with the necessary information as required under Articles 13 and/or 14 of the GDPR, including information about their data protection rights.

2. How concerned are you about not having complete control over the information you provide to organisations?

When prompted to consider how concerned they were over not having complete control over the information provided to organisations, almost 90% of the respondents expressed concern (i.e. 63.3% were fairly concerned and 25.8% were very concerned).

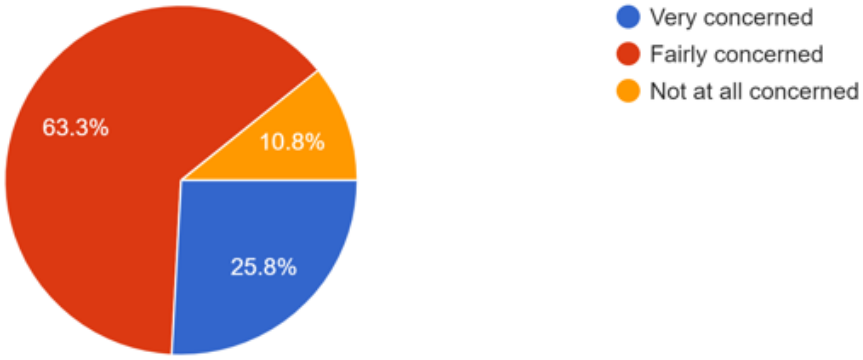


Illustration C – Level of concern over not having complete control of personal data provided to organisations

The results emphasise the importance of data protection to individuals, highlighting a significant concern where an individual does not have control over the information they provide to organisations. This result further illustrates the need for organisations to inform individuals about their data protection rights, as required by Article 13 of the GDPR. Realistically, if individuals are better informed about their rights, their concerns regarding their control over their data may diminish.

In addition to the need for organisations to provide individuals with information, the Commissioner considers that he may need to carry out further activities to raise awareness amongst the general public about the rights of individuals over their personal data.

3. Everyday activities are recorded in different ways.

The discussion now moves onto issues relating to the recording of people's everyday activities.

Respondents were asked to rate how concerned they were in relation to six specific data processing activities.

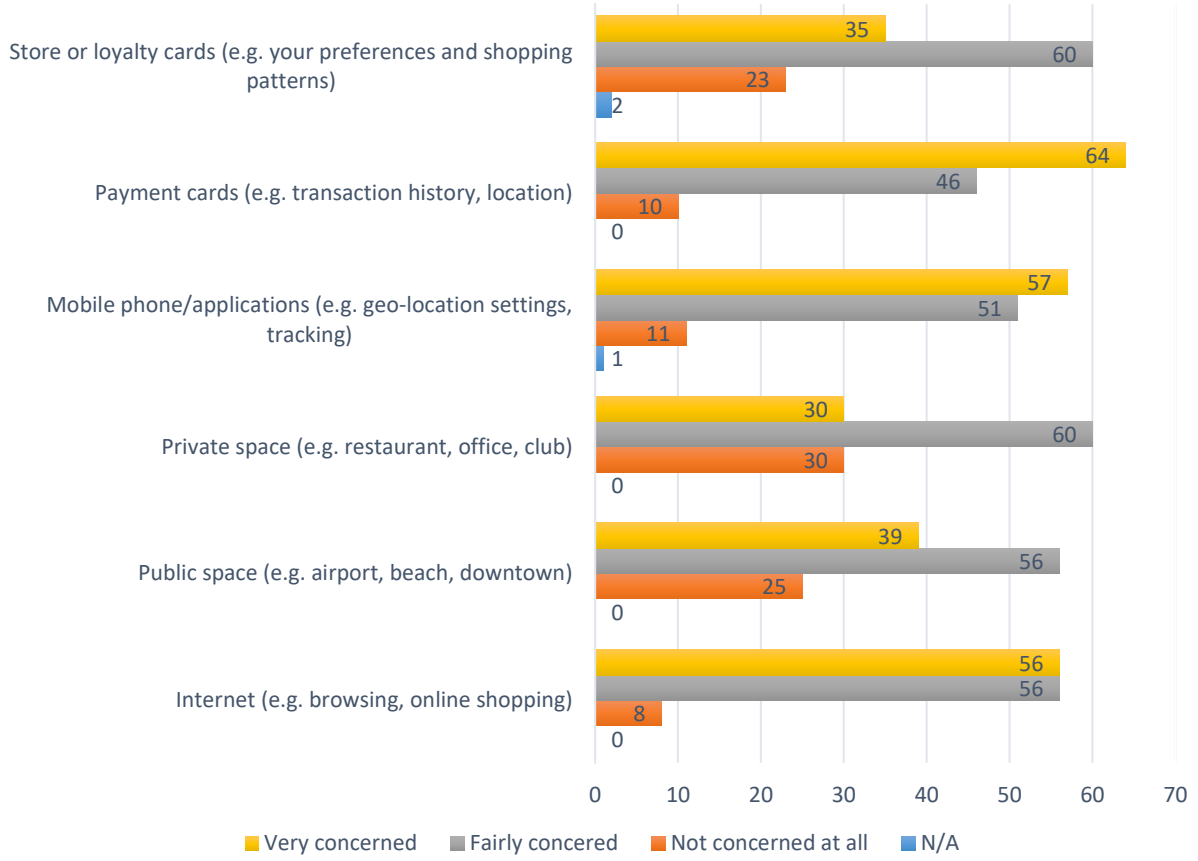


Illustration D – Recording of personal data

First and foremost, the results show that the public have concerns in regard to the recording of data in all areas, with the least concern arguably being the recording of everyday activities within private premises, such as restaurants.

The greatest concern exists in relation to the recording of transactions when using payment cards (e.g. transaction history, location) in which 64 respondents feel "very concerned" about this. However, when combining the results gathered from "very concerned" and "fairly concerned" responses, a total of 112 respondents perceived the Internet to be of greatest concern.

The list below identifies the six data processing activities listed by the activities that recorded the highest concern, when results for "very concerned" and "fairly concerned" were combined–

A. Internet (112 votes)
B. Payment cards (110 votes)
C. Mobile phone/applications (108 votes)
D. Public space (95 votes)
E. Store or loyalty cards (95 votes)
F. Private space (90 votes)

4. Public opinion in regard to the provision of personal data.

The majority of respondents believe that "*providing personal information is an increasing part*

of modern life" (102 votes) and that "*there is no alternative than to provide personal information […] to obtain products or services*" (90 votes).

However, the majority of respondents disagree with the statement that "*providing personal information is not a big issue*" (88 votes) and also disagree with "*providing personal information in return for free services online*" (72 votes).

The results show that the public recognises the increase in data processing in today's world, but equally show that they do care about the information they share with organisations, even when doing so in return for free services. Combined, the results highlight the importance of data protection to the public, particularly in an increasingly digital and data driven world.

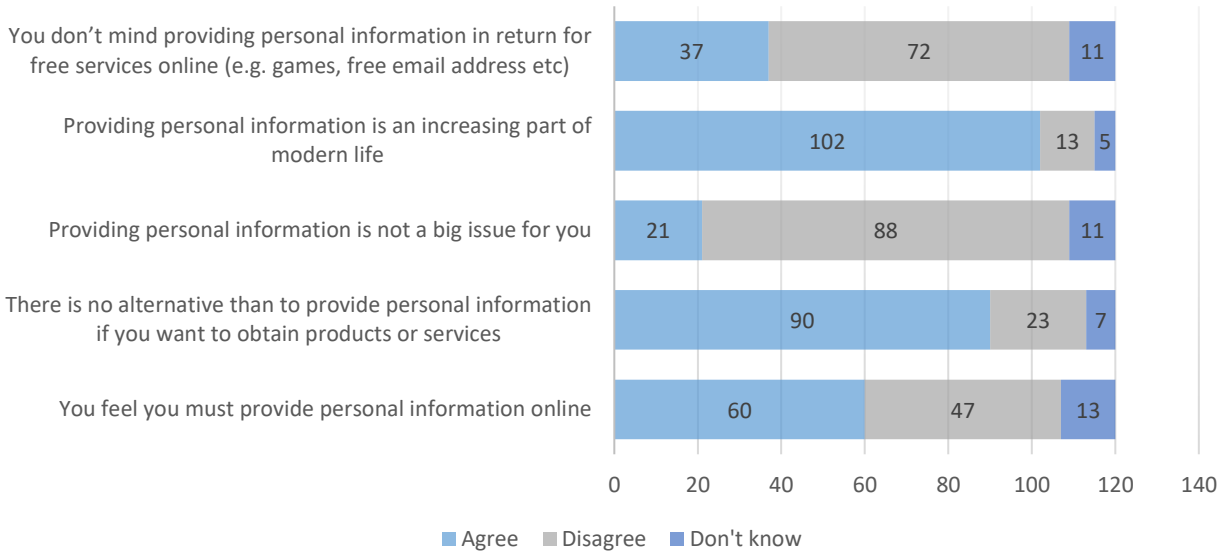


Illustration E – Public opinion in regard to the provision of personal data

5. Is consent required before personal information is collected and processed?

In the Survey, respondents were asked if they believed consent was required before their personal data was collected and processed. The results are illustrated in the following –

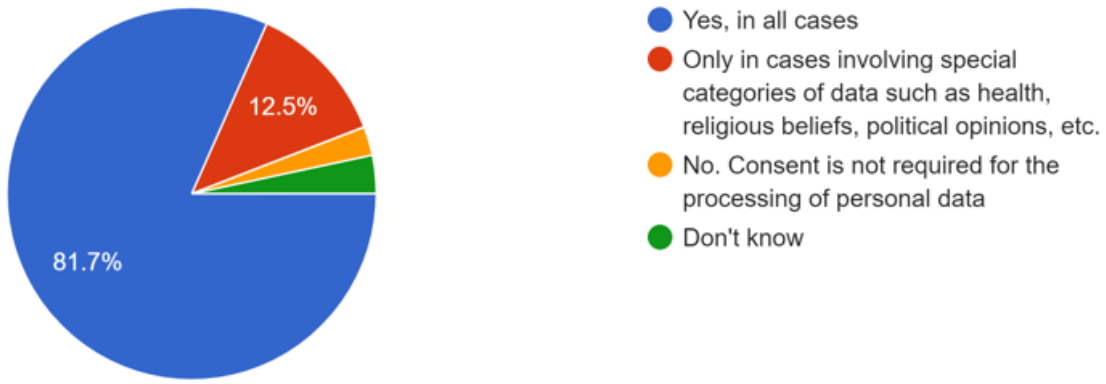


Illustration F – Requiring consent prior to processing personal data

A majority of respondents (81.7%) thought that consent should be required in all cases and a further 12.5% of the respondents stated that consent is only required in cases involving special categories of data. A minority of 2.5% consider that consent is not required for the processing of personal data and 3.3% of respondents chose not to select any of the aforesaid options.

Results show that the majority of respondents appear to believe that processing is legitimate only when consent is sought. It is important to note that consent is only one of the six lawful bases to process personal data under Article 6 of the GDPR. However, the Commissioner considers it perfectly reasonable for the layperson not to be technically aware of the various legal bases available for the processing of personal data under Article 6 of the GDPR.

It may also be that individuals relate consent with their awareness and control over what data processing takes place, which would again illustrate the importance of transparency in all cases.

6. Defined purpose for processing of personal information

Article 5(1)(b) of the GDPR states that "*personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes […]*". In practice, organisations must be clear from the outset about why they are collecting personal data and for what purpose they intend to process the data, without further processing.

In the Survey, respondents were asked whether they would be concerned if organisations used information about them for a different purpose than the one it was collected for, without prior notification and 75% stated they would be "*very concerned*" if this occurred.

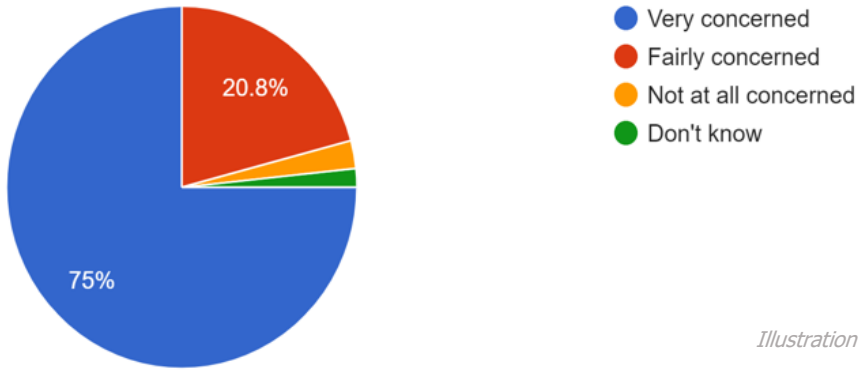


Illustration G – Defined purpose for processing

Only 2.5% of the respondents were "*not concerned at all*" and 1.7% said they did not know.

Specifying the purpose from the outset as well as establishing limits to the use of the data (i.e. purpose limitation), helps organisations comply with their accountability obligations. It will help organisations in their efforts to be transparent about their use of data and allow individuals to better understand said use. It is the Commissioner's view that this is fundamental to building public trust and, whilst the principle of purpose limitation aims to ensure that the data processing is in line with the reasonable expectations of the individuals concerned, there are clear links with other principles, such as fairness, lawfulness and transparency.

7. Would you want to be informed by the organisation which holds your personal data if this information has been lost or stolen?

When individuals trust an organisation with their personal information, they expect this information to be protected. There are, however, many risks to the security of personal data. For example, online attacks in the form of hacking or internal misuse of data (e.g. snooping) are a real concern to individuals and their personal data.

A majority of 96.7% of respondents stated that they would want to be informed by the organisation that holds their personal data in the event that said data is lost or stolen. The results highlight the value of transparency and communication in relation to data breaches.

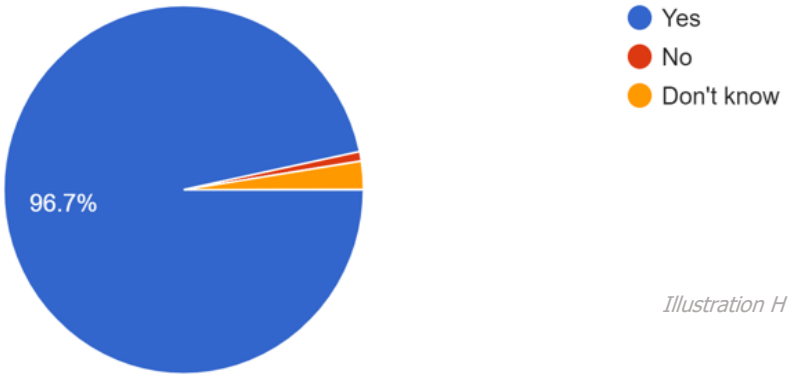


Illustration H – Notification to individual of data breach

Results show that only 1 respondent (0.8%) said they would not want to be notified of a data breach concerning their personal data and 3 respondents (2.5%) stated that they did not know whether they would want to be notified about a data breach.

8. Private sector v public sector.

Within the public and private sectors, organisations process vast amounts of personal data. For example, in the private sector, organisations operating online may collect and process transactions of millions of individuals world-wide. In the public sector, government offices collect and process personal data relating to all, or the majority of, Gibraltar residents. At times, processing activities may involve the use of new technologies, which bring many benefits but also raise new risks to the processing of personal data.

Through its work, the Commissioner's office has noted differences between the private and public sector's approach to data protection. As a result, the Survey included questions to learn about the public's perception in regard to the processing of personal data in both sectors.

The Survey asked the following question –

"When an organisation in the PUBLIC/PRIVATE SECTOR asks you to provide personal data, would you say that you are appropriately briefed and made fully aware about the way(s) your information may be processed?"

In their response, respondents were asked to rate the private and public sector by classifying their response as "Always", "Sometimes", "Never" or "Don't know". The results are illustrated below -

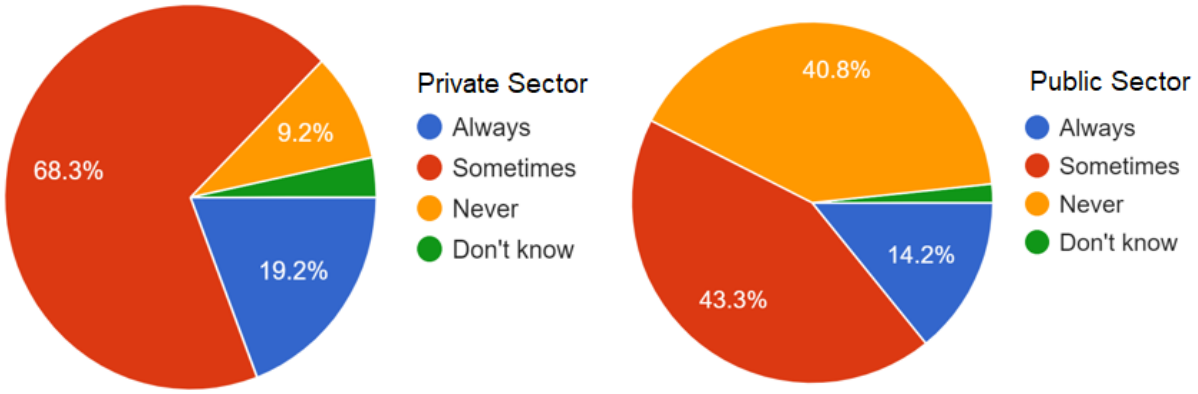


Illustration I – Private v public sector notification in regard to processing activities

Over 40% of the respondents claimed that the public sector "*never*" provides the appropriate information and are therefore not fully aware about the way(s) their information may be processed. Further, when combining the responses for "*always*" and "*sometimes*", 57.5% and 87.5% of the respondents classified the public sector and private sector, respectively, as appropriately providing individuals with the relevant information. The results clearly indicate that the public's experience and/or views in relation to the public sector are significantly poorer than that of the private sector.

The Survey also asked respondents to rate to what extent they trusted authorities and private companies to protect their personal information.

The results, as shown in Illustration J, illustrate that the majority of respondents tend to trust private companies over public authorities. The sector which respondents trust the most is that of "Private Legal Services" with the majority of votes under "*totally trust*", closely followed by Private Medical Services and Financial Institutions.

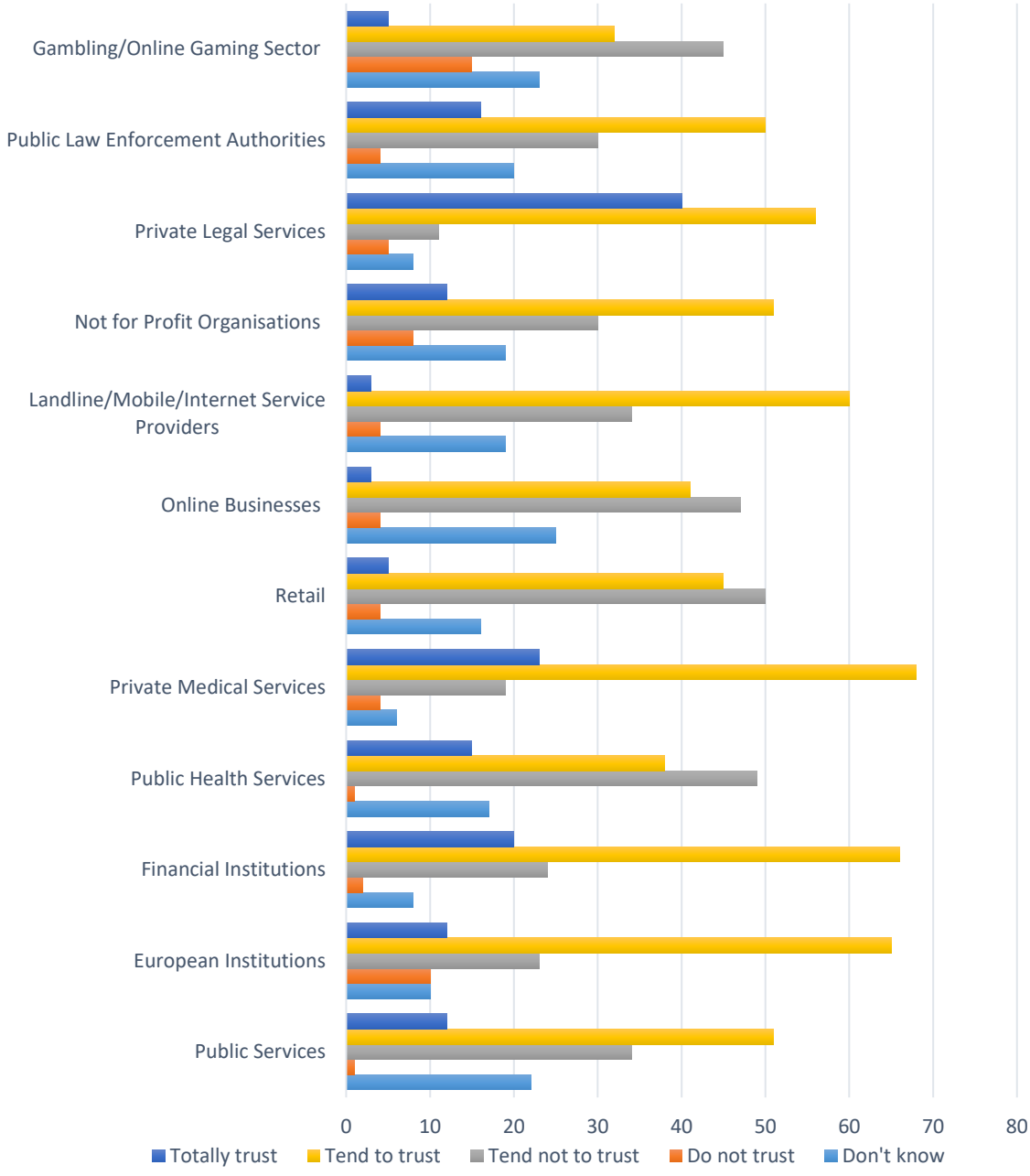


Illustration J - To what extent do you trust public/private authorities to protect your personal information

9. In terms of non-compliance with data protection law, what business types are perceived to be of most concern to the GRA?

Respondents were allowed to choose one or more answers to the above question and the majority of respondents deemed that the business type perceived to be of most concern to the GRA in terms of non-compliance with data protection law was "Health and medical institutions" with 70 votes totalling 58.3% of responses. This was closely followed by "Public sector bodies" with 66 votes.

Conversely, only 15 respondents consider "Not for profit organisations" (i.e. charitable organisations) to be of great concern to the GRA in terms of non-compliance with data protection law.

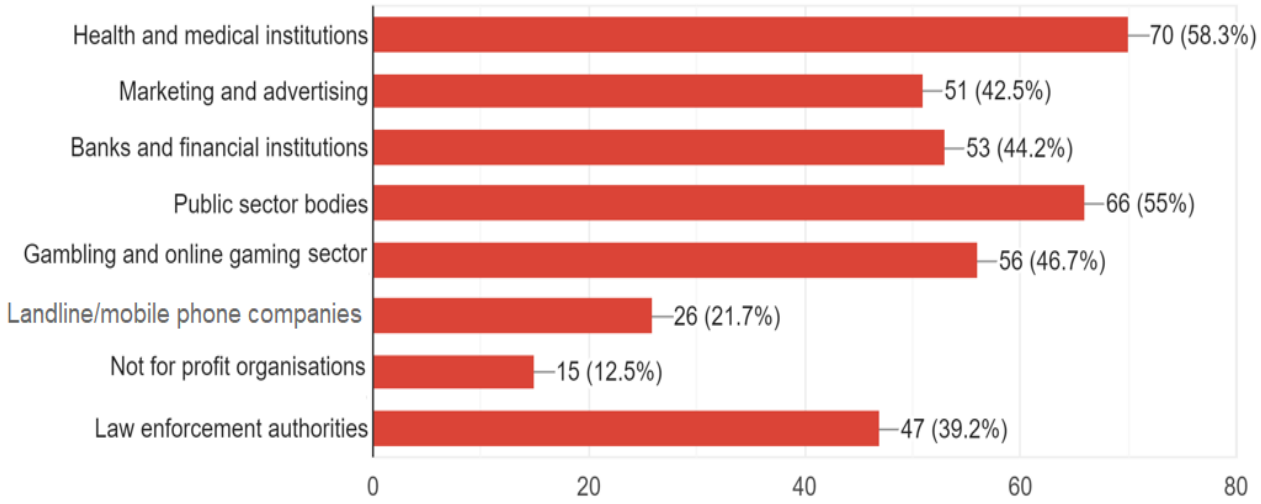


Illustration K – Business types perceived to be of most concern to GRA in terms of non-compliance with data protection law

10. What are the three most serious potential risks when providing an organisation with your personal information?

Respondents were asked to choose at least three preferred statements from the following -

- Information being shared with third parties without your consent
- Information being lost, stolen or unlawfully disclosed
- Absence of appropriate security measures in place
- Information being kept for a longer period than is necessary
- Information being used for other purposes without your knowledge
- Inaccurate information being kept about you
- Information being used to send unsolicited marketing
- No potential risks identified

Respondents deemed the following issues to be of greatest concern –

- Information being lost, stolen or unlawfully disclosed (87 votes)
- Information being used for other purposes without your knowledge (86 votes)
- Information being shared with third parties without your consent (78 votes)
- Absence of appropriate security measures in place (76 votes)

The potential risk which respondents were least concerned about was an organisation holding inaccurate data (13).

11. Public perception of the GRA.

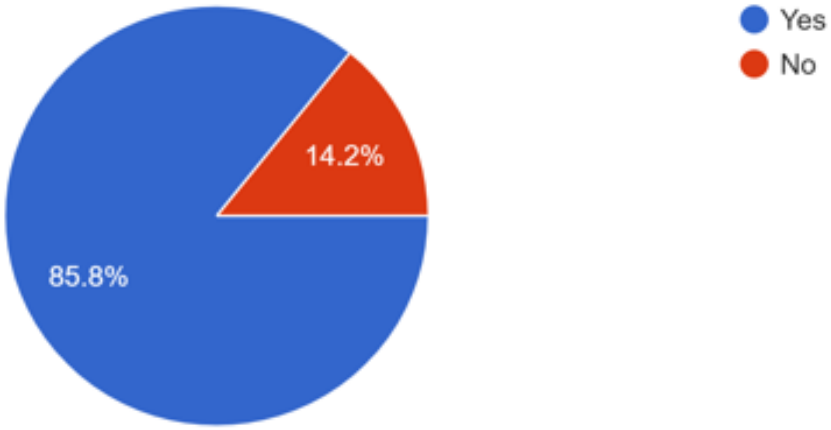
For several years now, guidance is an area that has been given greater priority by the Commissioner so as to assist organisations in their efforts to comply with the GDPR. So far, the Commissioner has published a total of 15 guidance notes to assist organisations in their understanding of the requirements of the GDPR. In addition, a series of data protection workshops have been organised, intended to promote collaboration and provide an open forum to debate data protection law and good practice.

The Commissioner's office also runs a parallel initiative, namely the "Control Your Privacy" campaign, that aims to raise awareness of data protection and the risks to privacy from digital technology so that individuals have sufficient knowledge and understanding to make informed decisions about the opportunities offered by said technology. This campaign further involves a combination of activities ranging from social media campaigns, e-newsletters, workshops, public awareness events and an awareness through education initiative, which involves school presentations and online resources for academics.

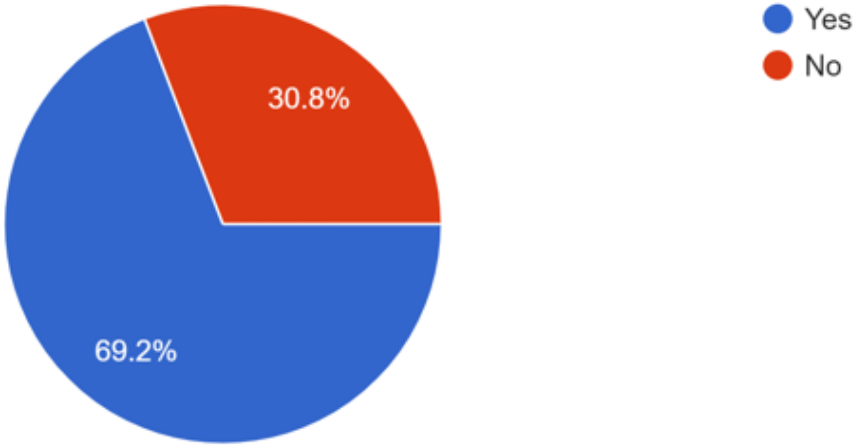
As part of the Survey, respondents were asked three questions in relation to the work carried out by the Commissioner's office. The aim of these questions was to learn about the views of the public in regard to the Commissioner's office and the work undertaken.

The questions and results gathered were as follows –

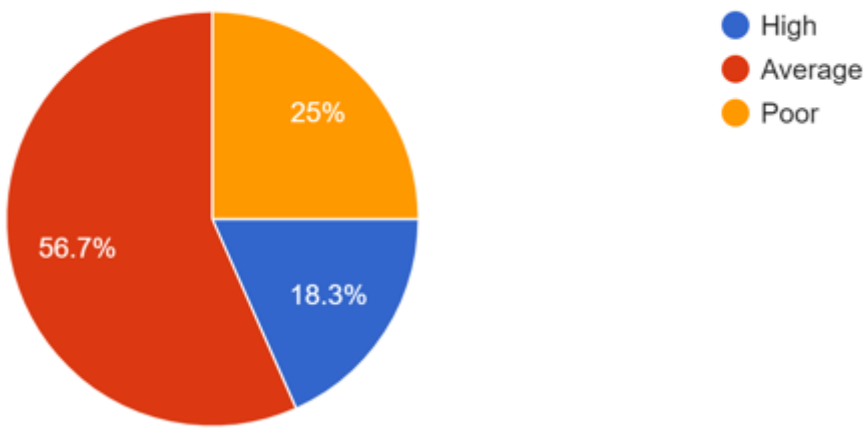
Did you know that the GRA is responsible for the enforcement of the Data Protection Act 2004 and the GDPR to uphold the rights of individuals and their privacy?



Are you aware that the GRA provide guidance on its website www.gra.gi, publishes weekly social media campaigns and issues a quarterly e-newsletter to subscribers with a view of increasing data protection awareness in Gibraltar?



What do you feel is the overall level of data protection awareness in Gibraltar?



CLOSING STATEMENT

The Commissioner reflects on the Survey's key findings in the following –

- Only one in ten individuals feel they have complete control over their personal data. 16.7% feel they have no control at all. The results are concerning given the introduction of the GDPR and its emphasis on enhancing the rights and control of individuals over their personal data.

- Nine out of ten individuals show concern about not having control over the information they provide to organisations, which highlights the importance of data protection to individuals.

- The results show that the public have concerns in regard to the recording of their data in all areas but showed the greatest concern when their data is used on the internet.

- The results show that the public recognises the increase in data processing in today's world, but equally show that individuals do care about the information they share with organisations, even when doing so in return for free services. Combined, the results highlight the importance of data protection to the public, particularly in an increasingly digital and data driven world.

- Three quarters of respondents stated that they would be "very concerned" if organisations used information about them for a different purpose than the one it was collected for. The result highlights the importance of ensuring that data is used in a transparent manner and in accordance with the expectations of individuals.

- Virtually all respondents expressed their wish to be informed about personal data breaches that affected their data, emphasising the importance of transparency and communication.

- The results clearly indicate that the public's experience and/or views in relation to the public sector are significantly poorer than that of the private sector.

- The sector which respondents trust the most is that of "Private Legal Services".

- Health and medical institutions were identified as the sector that should be of most concern to the GRA in terms of non-compliance with data protection law.