|  |
| --- |
| Close-up image showing the leaf-sides of two oversized books side-by-side on a bookshelf, with additional books in soft focus background |
| Wealth of Nations  Report |
| |  |  |  | | --- | --- | --- | | Angelica Vancea | 3/4/23 | GLA 3 Data Visualisation | |

# GLA 3 Data Visualisation

Table of Contents

[GLA 3 Assignment 1 Excel and Tableau 1](#__RefHeading___Toc4279_4185695687)

[First Task 2](#__RefHeading___Toc4281_4185695687)

[Policies and Procedures 2](#__RefHeading___Toc4283_4185695687)

[A. General Data Protection Regulation (GDPR) 3](#__RefHeading___Toc3176_41856956874)

[B. The Data Protection Act 2018 (DPA) 4](#__RefHeading___Toc3176_41856956873)

[C. The Freedom of Information Act 2000 7](#__RefHeading___Toc3176_4185695687)

[D. Electronic Communications Regulations 2003 8](#__RefHeading___Toc3176_41856956871)

[E. Investigatory Powers Act 2016 8](#__RefHeading___Toc3176_41856956872)

[F. The Computer Misuse Act 1990 8](#__RefHeading___Toc3178_4185695687)

[Second Task 9](#__RefHeading___Toc4285_4185695687)

[Excel 9](#__RefHeading___Toc4287_4185695687)

[1. Set a password to protect the workbook 10](#__RefHeading___Toc4515_4185695687)

[2. Change Data Type 10](#__RefHeading___Toc4517_4185695687)

[3. Insert a table 10](#__RefHeading___Toc4519_4185695687)

[4. Filter the data 10](#__RefHeading___Toc4521_4185695687)

[5. Create a chart 11](#__RefHeading___Toc4523_4185695687)

[6. Edit the chart 11](#__RefHeading___Toc4525_4185695687)

[7. Copy the chart 12](#__RefHeading___Toc4527_4185695687)

[8. Top 20 countries filter 13](#__RefHeading___Toc4529_4185695687)

[9. Top 20 countries Bar chart 13](#__RefHeading___Toc4531_4185695687)

[10. Colour the background 13](#__RefHeading___Toc4533_4185695687)

[11. Add a header 14](#__RefHeading___Toc4535_4185695687)

[12. Add a footer 15](#__RefHeading___Toc4537_4185695687)

[13. Save 16](#__RefHeading___Toc4539_4185695687)

[Third Task 16](#__RefHeading___Toc4289_4185695687)

[Tableau 16](#__RefHeading___Toc4291_4185695687)

[A. Import data 16](#__RefHeading___Toc4541_4185695687)

[B. Set relationships 17](#__RefHeading___Toc4543_4185695687)

[C. Check data types 17](#__RefHeading___Toc4545_4185695687)

[D. Build charts 18](#__RefHeading___Toc4547_4185695687)

[E. Client Requirements 18](#__RefHeading___Toc4293_4185695687)

[F. Built a dashboard 18](#__RefHeading___Toc4549_4185695687)

[Fourth Task 19](#__RefHeading___Toc4295_4185695687)

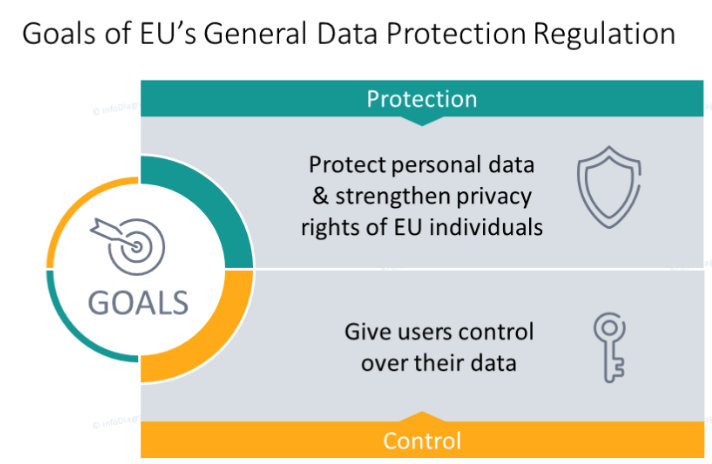
[Reflective 19](#__RefHeading___Toc4297_4185695687)

# First Task

## **Policies and Procedures**



After Google-ing “GDPR patterns”, I was able to find an application, named **Varonis**, which automatically identifies and classifies GDPR data with over 340 exclusive patterns that cover all 28 EU countries. These patterns and classifications help organisations automatically classify GDPR data, build out security policy to monitor, and alert on GDPR affected data. One organisation found over 10,000 files which included information like bank account numbers, credit card numbers, and international bank account (**IBAN**) numbers across five different EU countries. **Ardoq**, is another application to help with compliance as it helps companies track progress, visualise gaps and their severity, and selectively share data across the organisation.

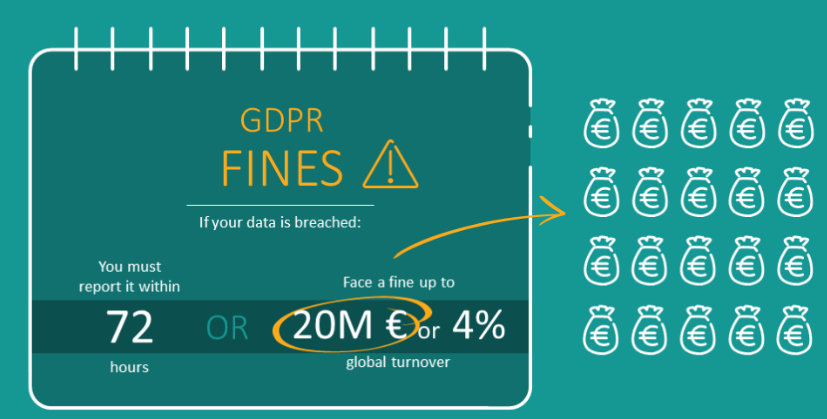
****

## **A. General Data Protection Regulation (GDPR)**

In the United Kingdom, the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA) set out the policies that organisations must follow when working with personal data. These laws apply to organisations operating within the European Union (EU), as well as those outside the EU if they process personal data of individuals in the EU.

The main principles of the GDPR include:

1. Lawfulness, fairness, and transparency: organisations must have a lawful basis for processing personal data, such as obtaining the individual's consent.
2. Purpose limitation: organisations must collect personal data for specific, explicit, and legitimate purposes, and not further process it in a manner that is incompatible with those purposes.
3. Data minimisation: organisations must only collect and process the personal data that is necessary for the purpose it was collected for.
4. Accuracy: organisations must ensure that personal data is accurate and kept up-to-date.
5. Storage limitation: organisations must not store personal data for longer than is necessary for the purpose it was collected for - data can be kept for longer as long as anything that identifies the individual is removed.
6. Integrity and confidentiality: organisations must implement appropriate technical and organisational measures to ensure the security of personal data.



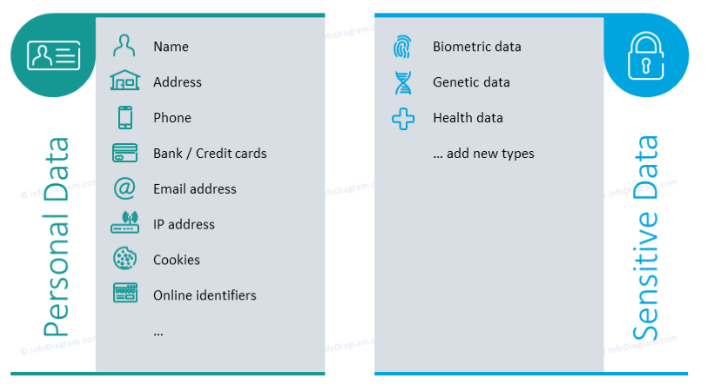
## B. The Data Protection Act 2018 (DPA)

The Data Protection Act 2018 (DPA) sets out additional provisions specific to the UK, such as the right for individuals to make subject access requests to obtain a copy of their personal data that an organisation holds about them.

GDPR differs from the Data Protection Act of 1998/2018 by also including ‘the right to be forgotten’, which means that an individual can request that an organisation erases all their personal data. This right only applies in certain circumstances.

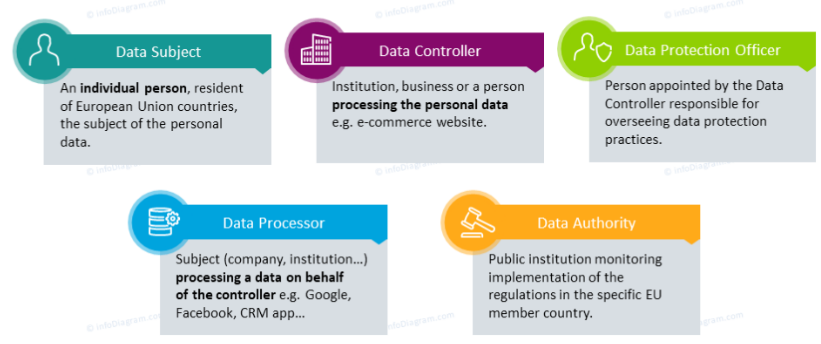
The Data Protection Act 1998/2018 exists to protect personal details. This personal data includes items such as:

* name and address
* date of birth
* medical records
* school and employment records
* religion



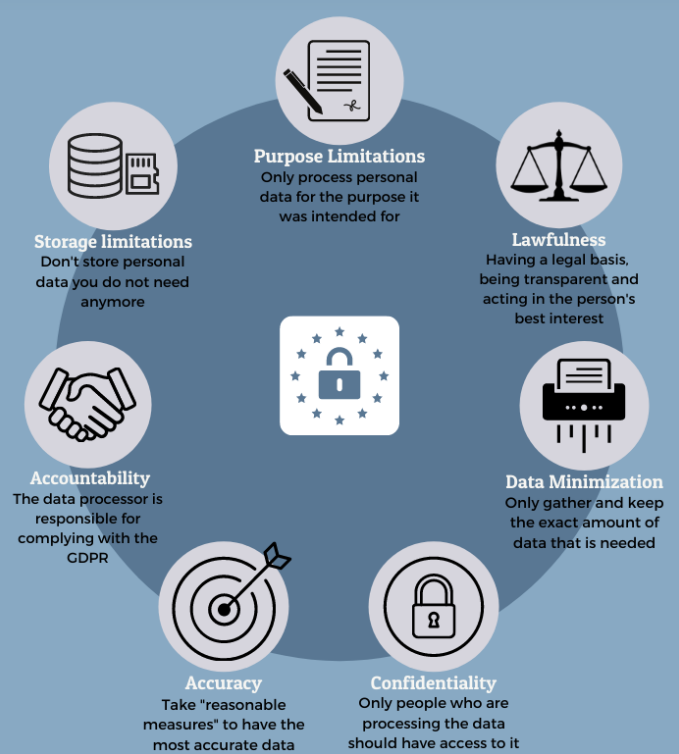
A person who has data stored about them is known as a data subject. As a data subject, a person has the right to see what data is held about them by an organisation and to have that data amended if incorrect.

Every organisation that holds data must appoint a data controller. This person is responsible for ensuring that the organisation stays within the principles stated by the Data Protection Act.



The Data Protection Act is built around eight principles (rules) which state how personal data should be treated:

1. Personal data must be fairly and lawfully processed. This means that an organisation must be truthful about what personal data they wish to collect and what they want to use it for.
2. Personal data must be obtained for specified and lawful purposes. This means that an organisation cannot use personal data for any purpose other than that stated when they collected the data. For example, if a company wanted your exam records to see if you were qualified for a job, it could not use those records to try to sell you revision guides that it thinks you might need. Also, the company cannot pass on your data to any other organisation without your permission.
3. Personal data must be adequate, relevant and not excessive. This means that an organisation cannot ask for any data that is not needed. For example, when you apply for a bank account the bank cannot ask you where you went on holiday last year.
4. Personal data must be accurate and up to date. If data held about you is wrong or out of date, you have the right to have it corrected or deleted. This is extremely important, as incorrect or out-of-date data might, for example, prevent you from getting a job or a loan, or being able to buy a house.
5. Personal data must not be kept for longer than is necessary. As soon as an organisation no longer needs your data, they must delete it.
6. Personal data must be processed in line with your rights. This includes the right to see any data held on you and the right to correct inaccurate data.
7. Personal data must be held securely. This means that data must be kept safe from unauthorised access - for example, with usernames and passwords - but also safe from accidental loss - by making backups.
8. Personal data must not be transferred to other countries outside the European Economic Area unless those countries have similar data protection laws.



In the UK, the Data Protection Act is overseen by the Information Commissioner's Office (ICO). This is an independent regulatory authority whose responsibility is to see that organisations follow data protection legislation. The office has the authority to prosecute and fine any organisation found to be in breach of the Data Protection Act.

In January 2023, Information commissioner John Edwards has defended his new strategy for enforcing the UK GDPR with public sector bodies, using reprimands rather than fines. The Commissioner stated that fines to public bodies created a “money go-round” where funds were being moved between government organisations. Also, unlike in the private sector, fines do not come out of shareholder pockets or profits but come directly out of funds that are used to deliver services to the public. Citing an example where a fine was to be issued to an NHS Trust, he argued that this loss of funds would harm the quality of care provided to patients and thus further punishing victims whose rights the ICO should uphold.



On 17 November 2022 the Information Commissioner’s Office (ICO) published much needed  guidance on international data transfers alongside a Transfer Risk Assessment (TRA) tool.  The ICO has become the first regulator to provide step-by-step instructions for a transfer risk assessment. Given the impact of the Schrems II decisions, this is a useful move, that increases clarity for practitioners in this area. The ICO are also planning on publishing worked examples of assessments completed using the TRA to give more clarity on how the tool should be applied.

## C. The Freedom of Information Act 2000

The Freedom of Information (FOI) Act 2000 was introduced to give the public the right to access any information recorded by public sector organisations. These organisations include:

* schools
* councils
* government departments
* health trusts and hospitals
* libraries
* museums

Anyone is able to request information, regardless of how old they are, where they live or their nationality.

Requests must be made in writing, either by letter or by email. The organisation then has 20 working days to provide the information.

Many people incorrectly assume that public bodies must give them any information that they request. Organisations are excluded from providing information in the following cases:

* If the information required is regarded as sensitive - the Data Protection Act 1998/2018 and General Data Protection Regulation 2018 overrule in this instance. For example, a request to find out how much an employee earned would be rejected as that information is sensitive to the employee.
* If the information will be too costly or time consuming to produce. For a public organisation, such as a school or a council, the cost limit is £450. For example, if organisations determine costs based on £25 per hour per person and the information requested would take longer than 18 hours (18 × £25 = £450) to produce, the request would be rejected. For the government and armed forces, this limit is raised to £600 (24 hours).

## D. Electronic Communications Regulations 2003

Organisations in the UK must also comply with other legislation related to data protection, such as the Electronic Communications Regulations 2003 and the Privacy and Electronic Communications (EC Directive) Regulations 2003, which relate to electronic marketing communications.

Many smartphone apps ask for permission to access data held on the device. Once accessed, this data is usually sent to the app producer, who is often in another country and not always subject to the privacy laws that exist in the UK.

## E. Investigatory Powers Act 2016

In 2016, the government introduced the Investigatory Powers Act. This sets out rules on the use of investigatory powers by law enforcement and the security and intelligence agencies. Under the act, phone companies and internet service providers are required to keep copies of users' emails and browsing histories for a period of time. It also gives the police and security services the authority to access computers and phones to search for data. This act has proved controversial, with opponents concerned over how it impacts people's right to privacy.

## F. The Computer Misuse Act 1990

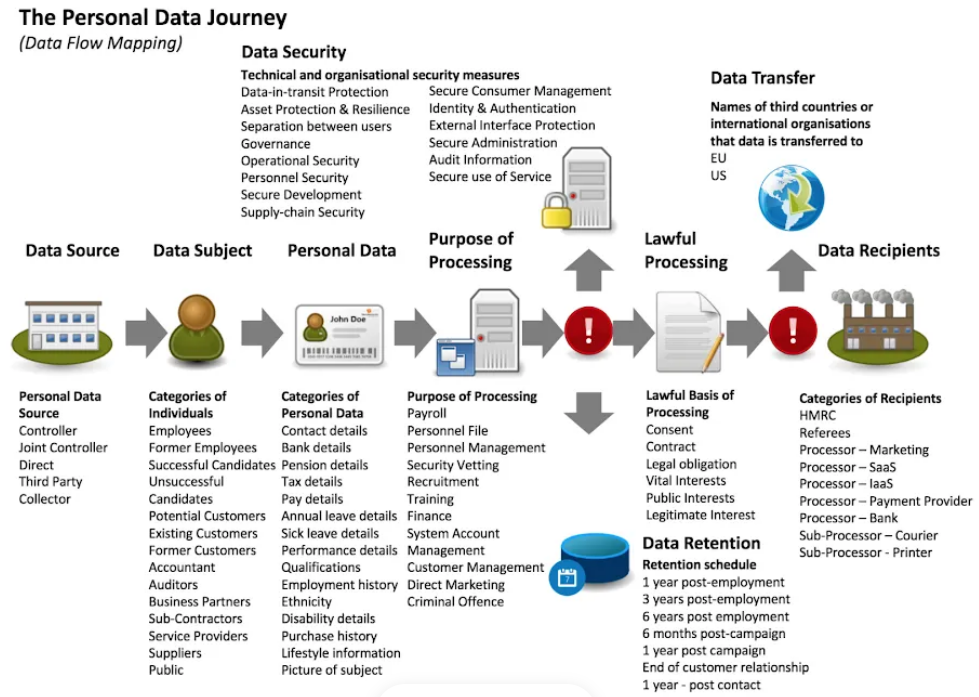
The widespread use of computers has led to new types of crime. The Computer Misuse Act 1990 attempts to discourage people from using computers for illegal purposes. There are three separate parts to the Act:

* It is illegal to access data stored on a computer unless you have permission to do so. Unauthorised access is often referred to as hacking.
* It is illegal to access data on a computer when that material will be used to commit further illegal activity, such as fraud or blackmail.
* It is illegal to make changes to any data stored on a computer when the user does not have permission to do so. If you access and change the contents of someone’s files without their permission, you are breaking the law. This includes installing a virus or other malware that damages or changes the way the computer works.

Punishment for breaking this law includes unlimited fines, several years in prison or both depending on the how severe the offence is.

However, one key part of the law is that intent must be proved. If a computer is not well protected, someone could accidentally access its data without meaning to. They might also accidentally change a document without realising it. For anyone to be found guilty, it has to be shown that they intentionally accessed and changed data.

In Europe, governance around AI and machine learning replaced incident management as a top priority. This is likely a response to new and forthcoming regulatory instruments like the Digital Services Act, AI Act, Digital Markets Act, Data Act and Data Governance Act that seek to provide stronger protection and better governance in relation to emerging technologies.

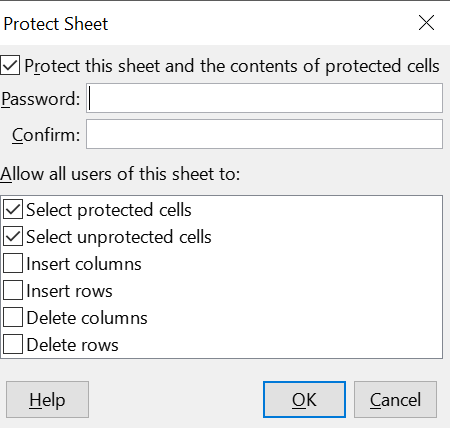
From <https://medium.datadriveninvestor.com/the-single-most-important-change-in-data-privacy-regulation-in-20-years-gdpr-b9026b9acfa9>

# Second Task

## **Excel**

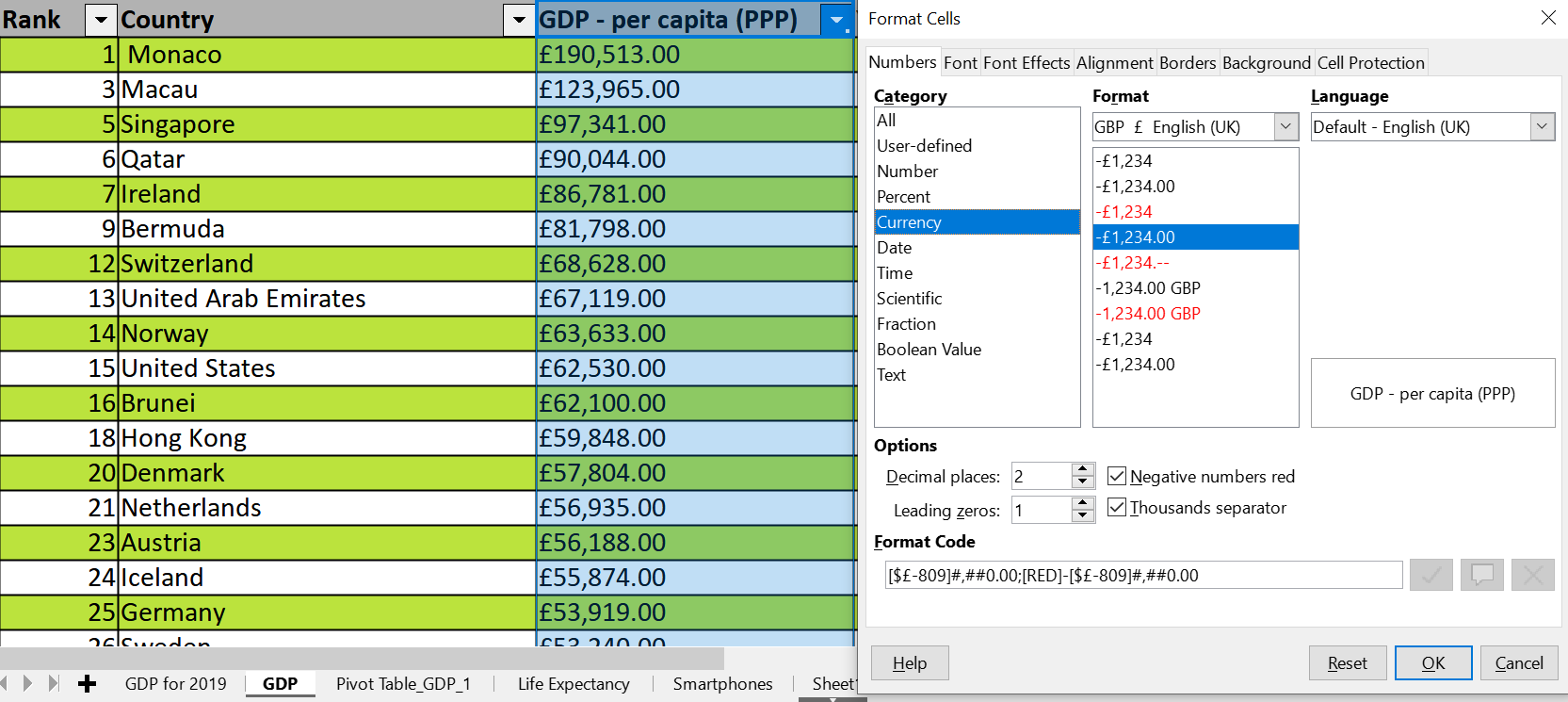
**GDP Tasks**

## Set a password to protect the workbook



## 2. Change Data Type

Highlight column C and change the data to display in British Pound symbol

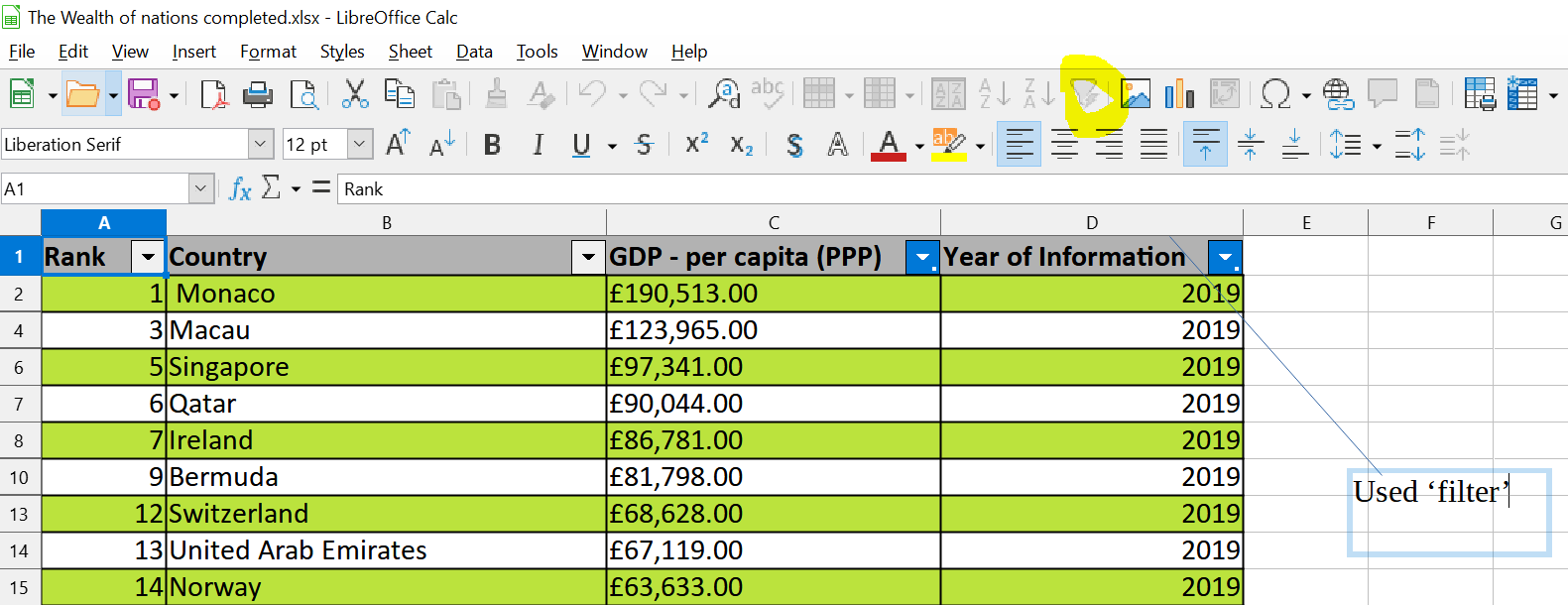


## 3. Insert a table

I selected the cells and used ctrl+T to turn the GDP sheet into a table.

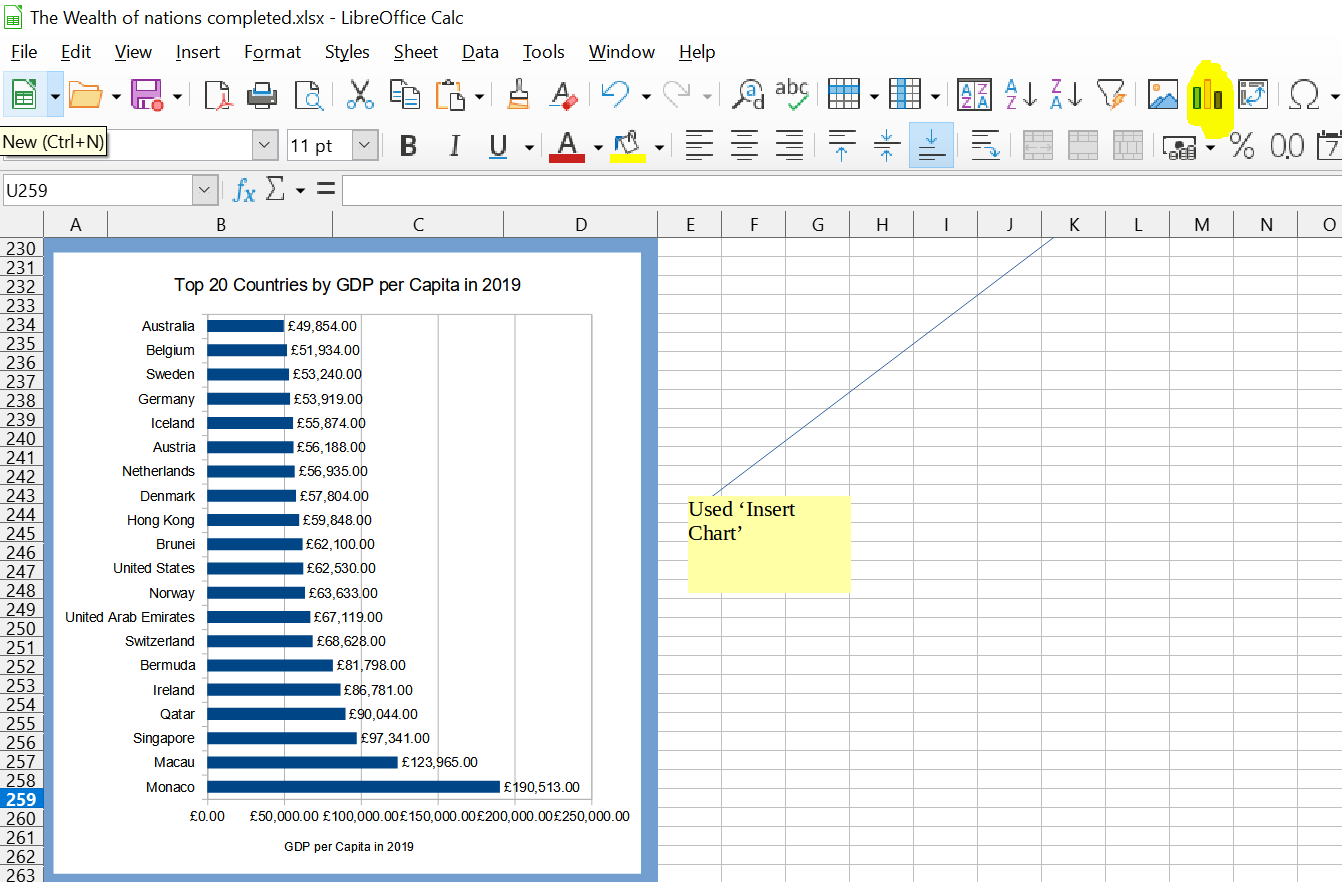
## 4. Filter the data

I have filtered the table to display only the information for 2019



## 5. Create a chart

Next create a chart that will only display the following data ‘Country and GDP - per capita (PPP)’. The chart can be anything as long as it is suitable.



## 6. Edit the chart

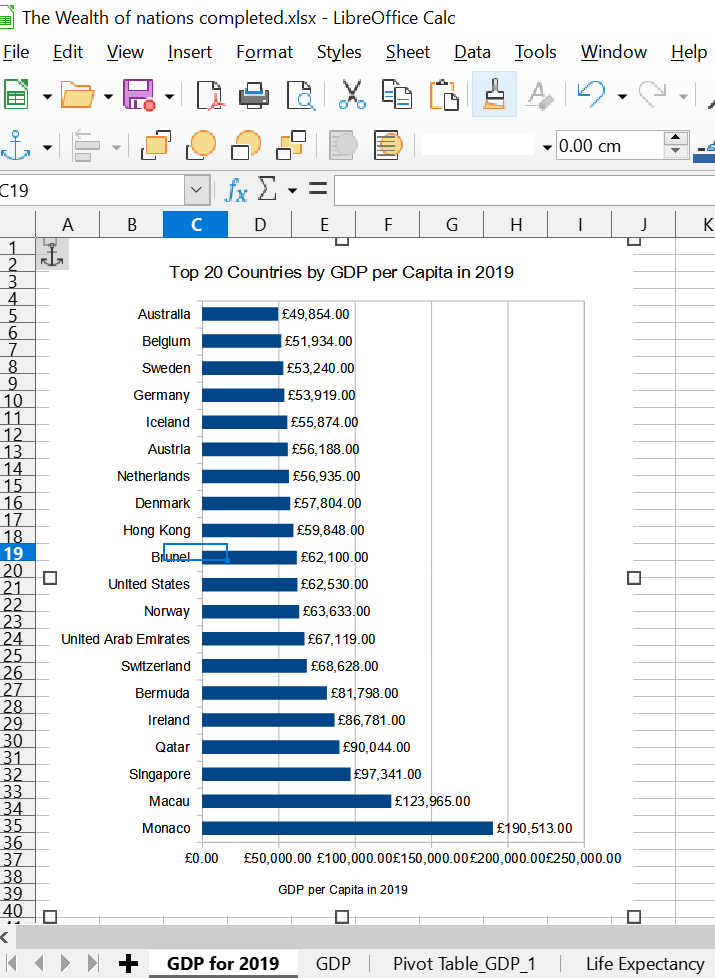
* + Add a title
  + Add X and Y axis labels
  + Make the chart visually pleasing



## 

## 7. Copy the chart

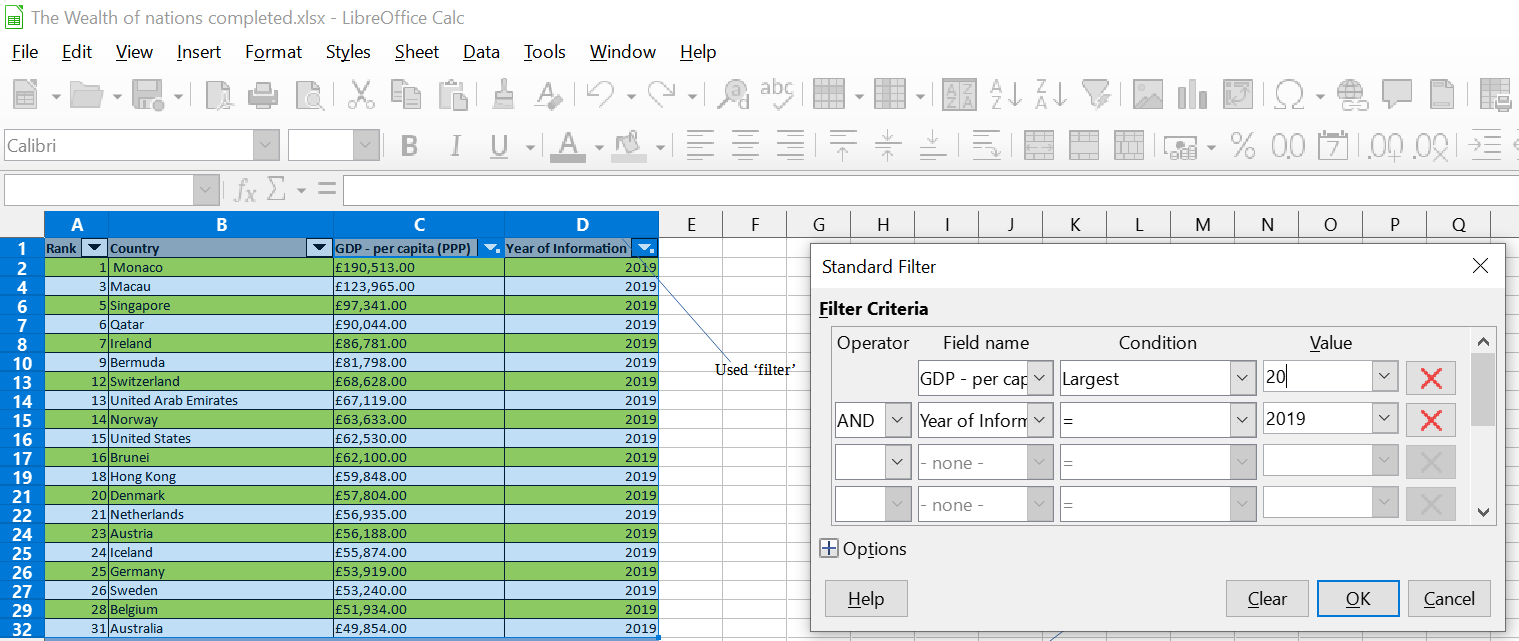
Move the chart to a new sheet tab and label with a suitable name



8.

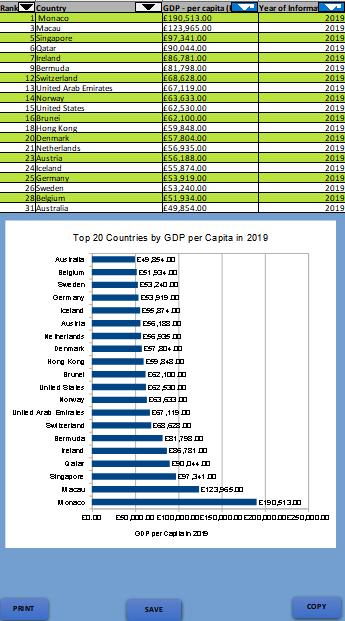
## 8. Top 20 countries filter

I have created a filter for the top 20 highest ranking countries in 2019.



## 9. Top 20 countries Bar chart

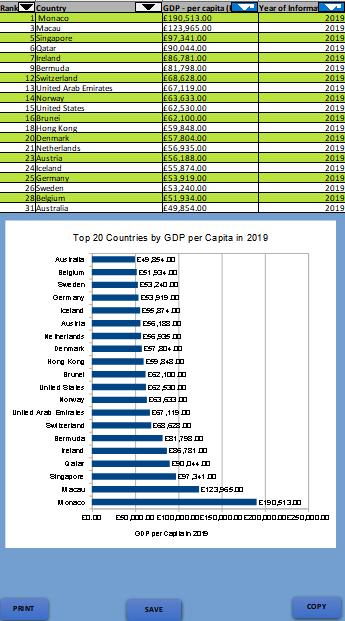
Next I created a new Bar chart to display the 20 highest ranking countries and then moved the chart to be underneath the table, as shown below.



## 10. Colour the background

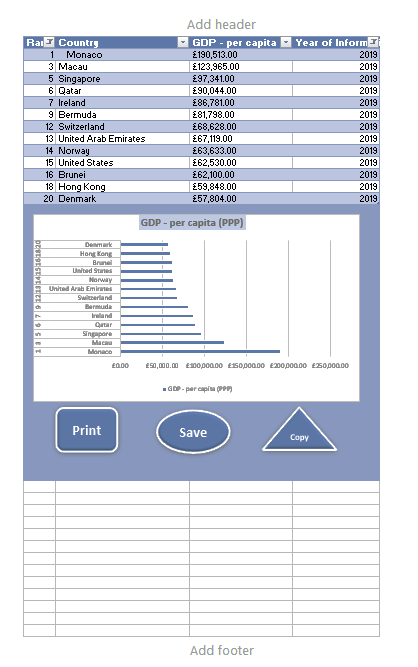
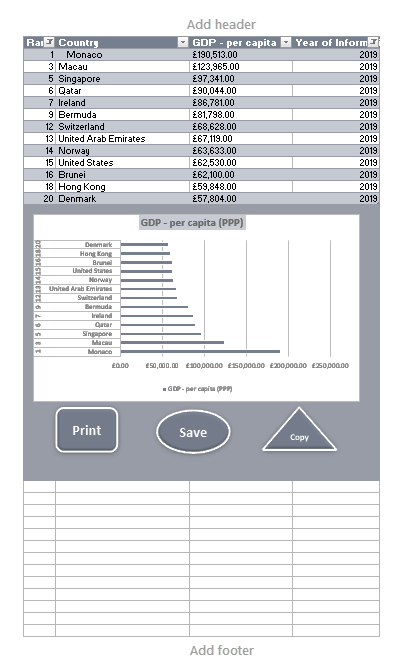
Find the ‘add a fill colour’ icon and select a colour, after highlighting the area underneath the table as shown below.

Graphical user interface, application

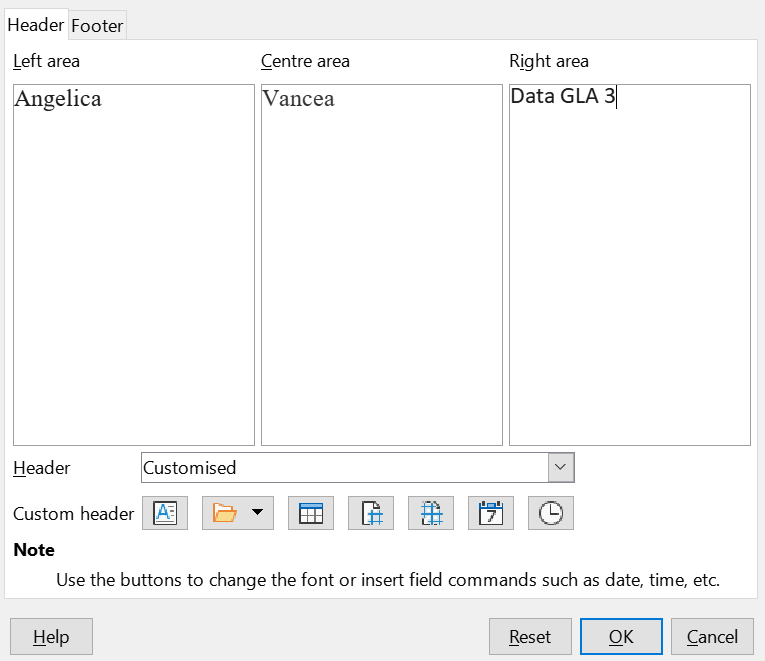
Description automatically generated

## 11. Add a header

Select the ‘Page Layout’ icon . This will then display the screen with a header and footer as seen below.

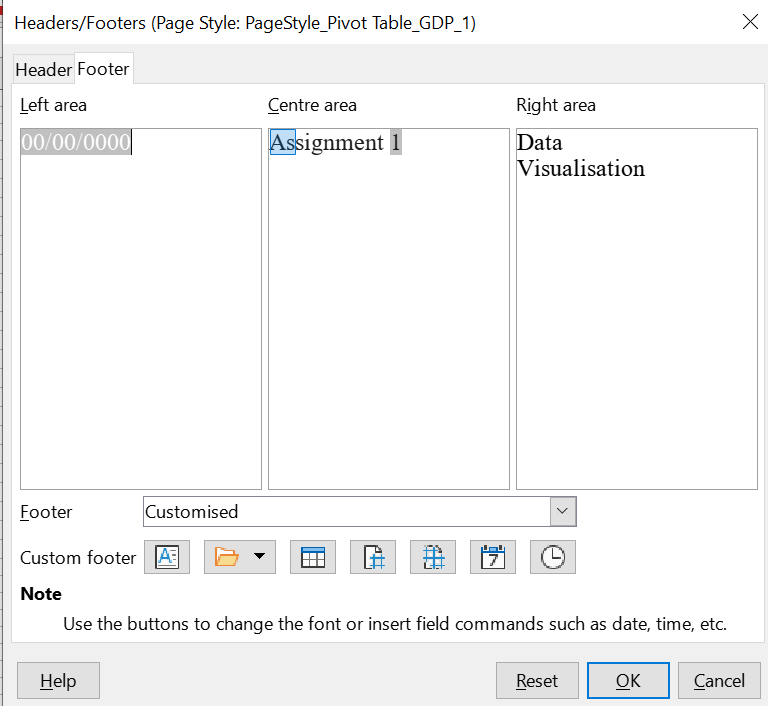


In the header I entered my name and GLA DATA 3 in the three boxes**:**



## 12. Add a footer

In the footer I added date, then Assignment 1 and lastly Data Visualisation.



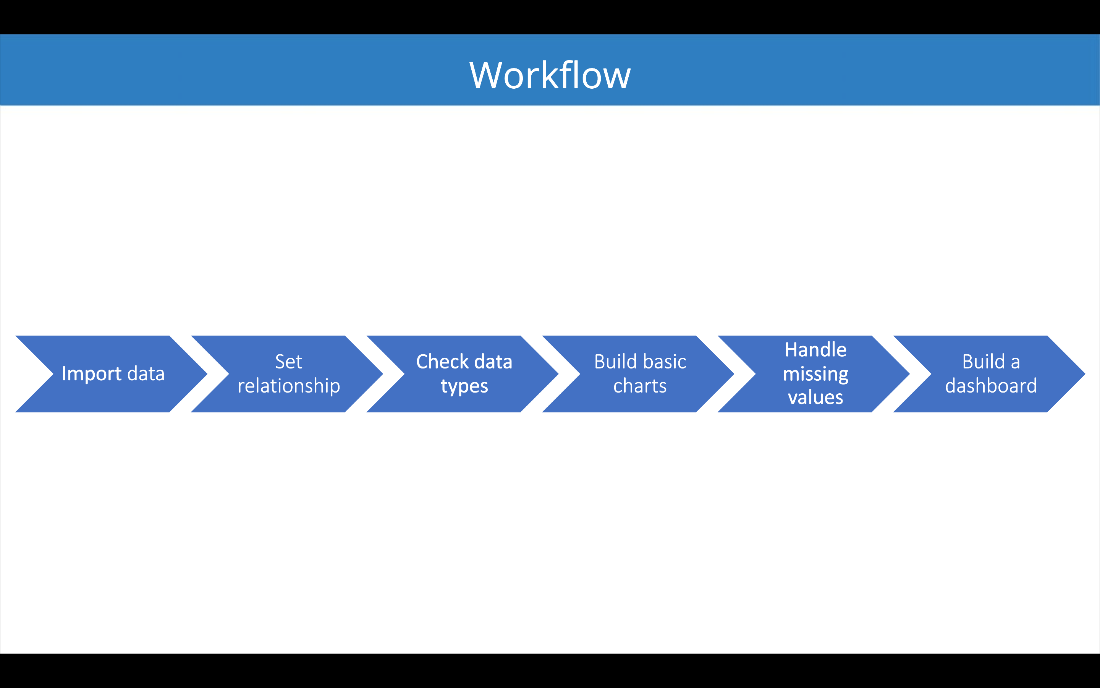
## 13. Save

Saved and closed my Excel document only.

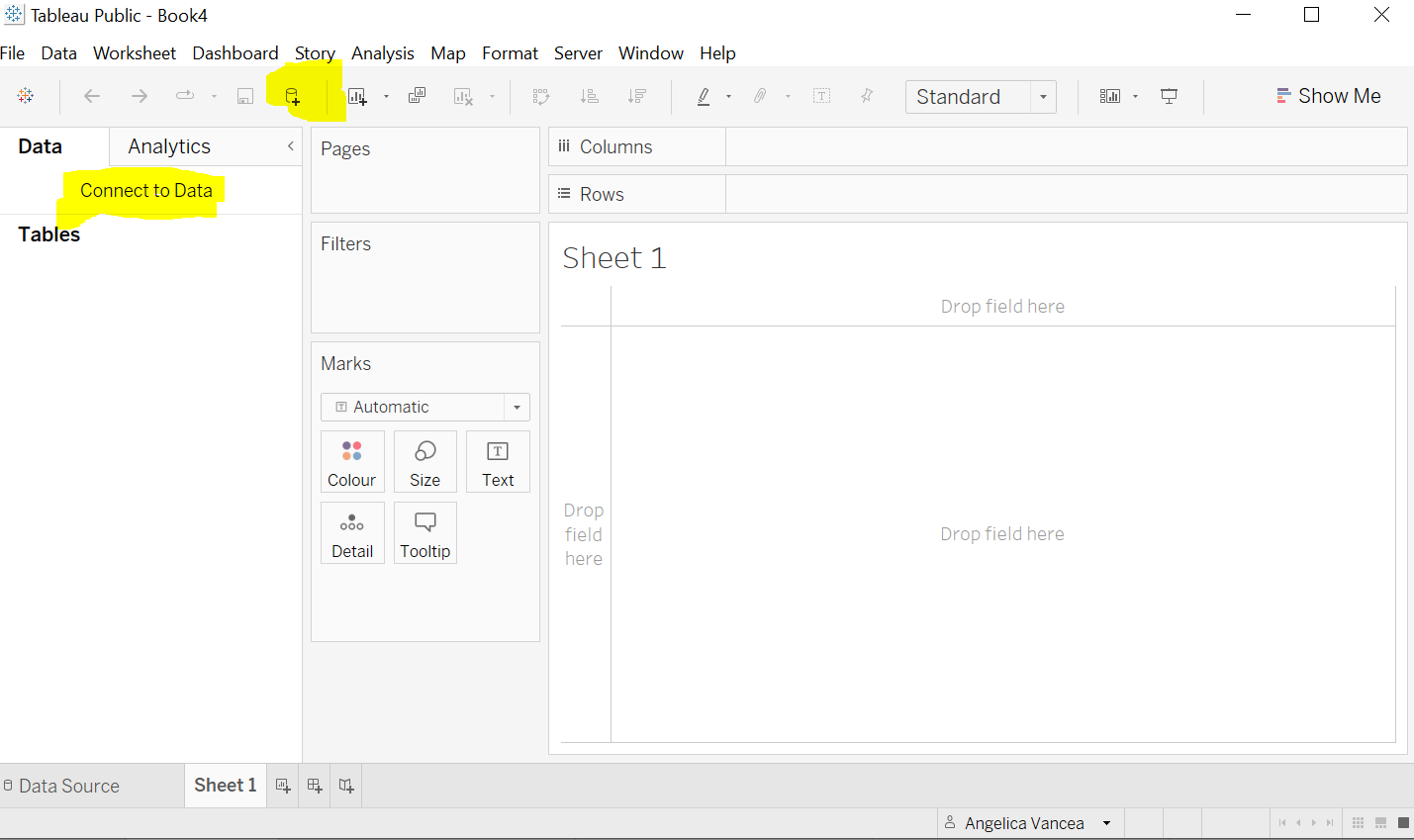
# Third Task

## **Tableau**

I have followed the workflow that we used in the workshop, as seen below:

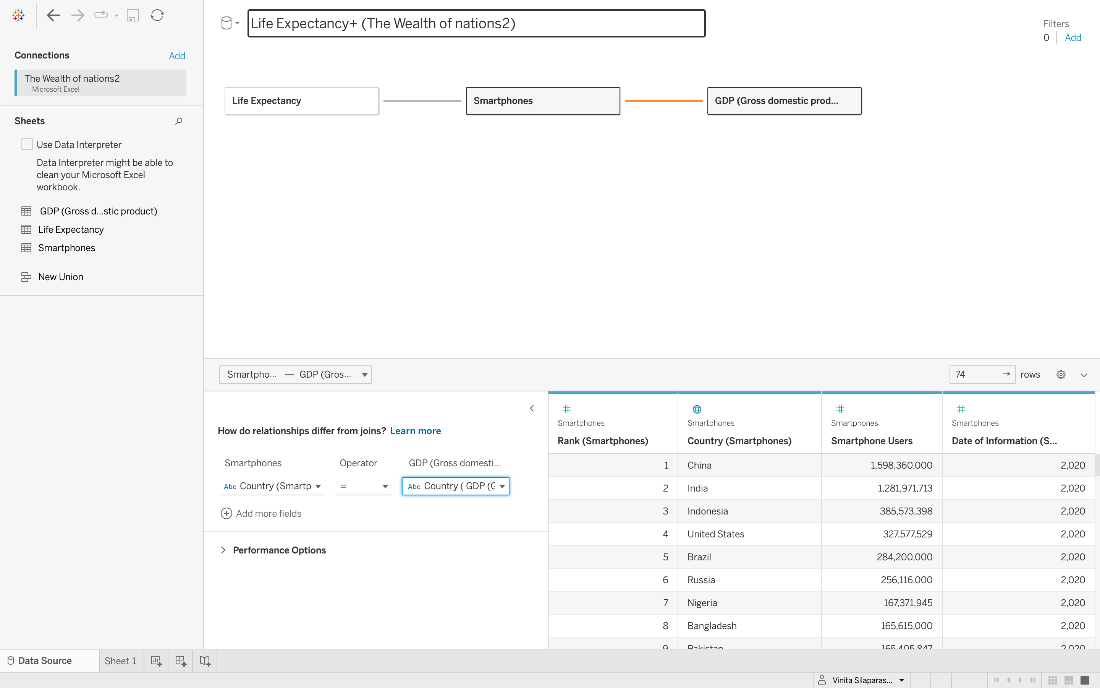


## A. Import data

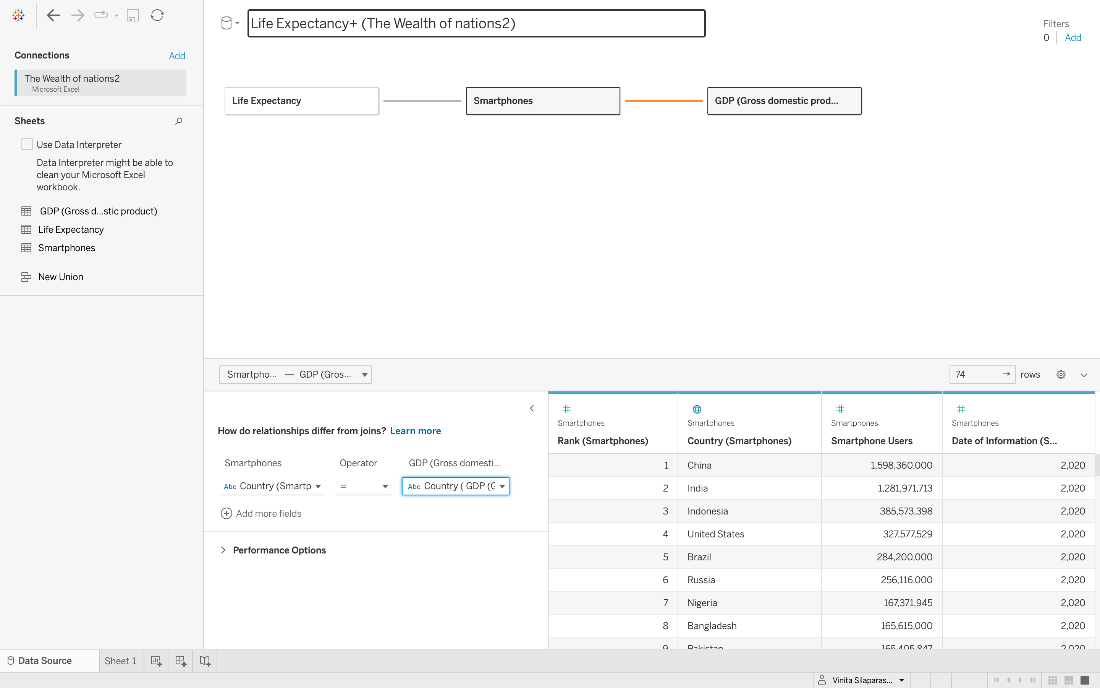


## 

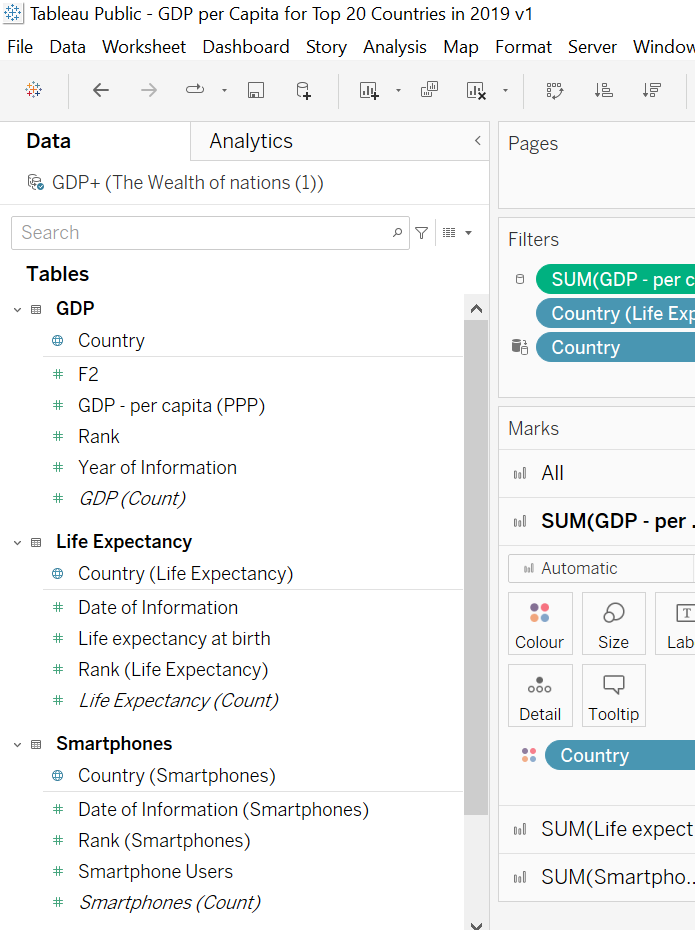
## B. Set relationships



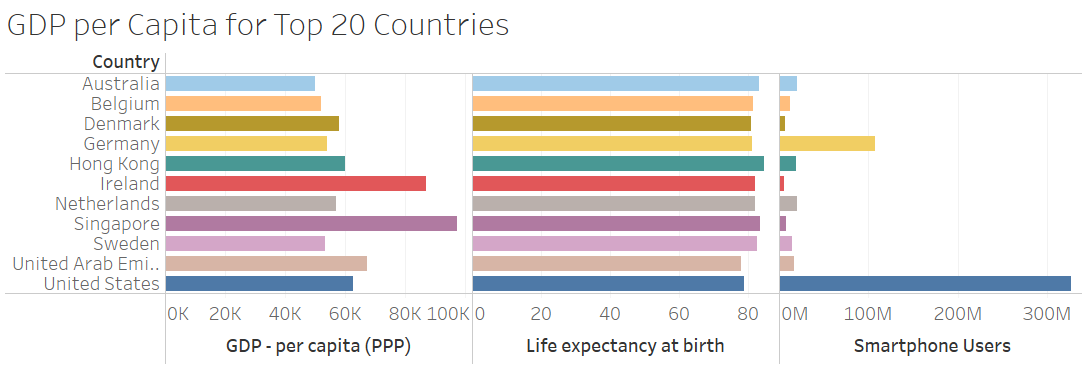
You have three sheets and the common column for all of them is country, so the visual arrangement of the sheets does not matter Only the columns that you use to create the relationship matters. You can arrange the sheets in a straight line as seen below:



## C. Check data types



## D. Build charts

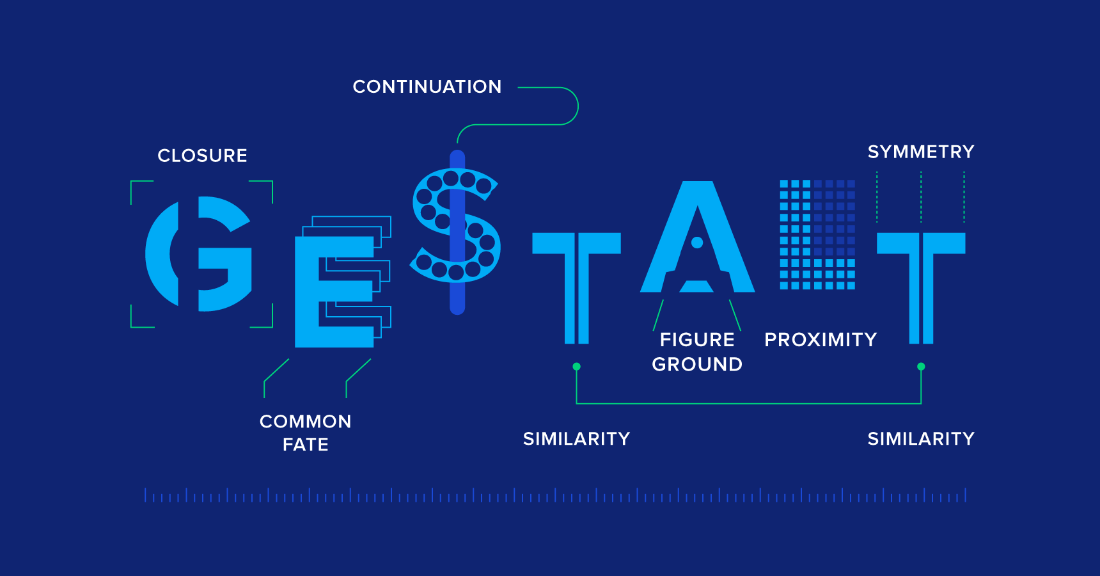


## **E. Client Requirements**

The client is colour blind so I have used the colour blind Palette when building my dashboard. The client is only interested in the top 20 highest ranking countries. All my visuals have been created only for the top 20 highest ranking countries.

## F. Built a dashboard

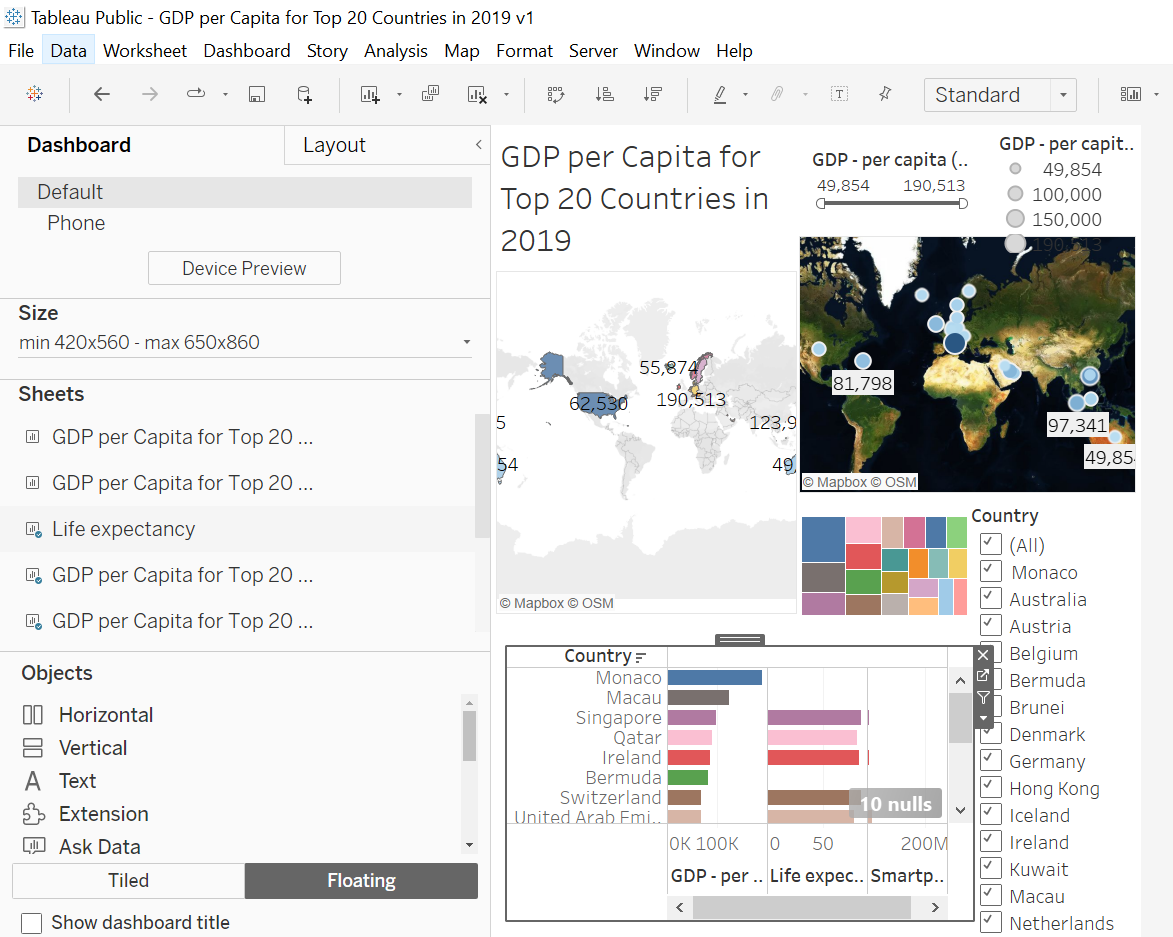
Gestalt principles have been a great guideline when creating my visuals.



Source: <https://www.toptal.com/designers/ui/gestalt-principles-of-design>

**Here is the link to my dashboard in Tableau:**

[**https://public.tableau.com/shared/YBN3QTPMS?:display\_count=n&:origin=viz\_share\_link**](https://public.tableau.com/shared/YBN3QTPMS?:display_count=n&:origin=viz_share_link)

****

# Fourth Task

## **Reflective**

The data used for the report was obtained from the World Bank’s website, and was broken down into individual countries. It included information such as the number of smartphone users, the life expectancy and GDP per capita. By comparing and contrasting these different metrics, important insights regarding the countries’ economic standing were revealed.

This report will discuss what was learned from making a Tableau dashboard about the top 20 countries by GDP per person in 2019. Through creating the report, key insights regarding each country’s GDP were revealed, as well as trends that could be observed when comparing different countries. Additionally, time was spent exploring and understanding the data to ensure the accuracy of the report, and to understand the correlations between various countries’ GDP.

Overall, there is a general positive **correlation** between life expectancy and GDP per capita, with most of the countries in the top 20 for life expectancy also having relatively high GDP per capita. However, there are some outliers, such as the United States, which has a relatively high GDP per capita but a lower life expectancy compared to other countries in the top 20. It is also worth noting that there are significant differences in the levels of GDP per capita among the top 20 countries, with some countries such as Switzerland and Ireland having much higher levels of income compared to others like Belgium, Kuwait and Australia.

The Tableau report also revealed a number of interesting **trends**. For example, countries in North America and Western Europe generally had higher GDP per capita than those in Asia, Africa, and South America. Additionally, the report revealed that countries with larger populations tended to have lower GDP per capita, which could be attributed to the fact that the resources of these countries are spread more thinly than in those with smaller populations.

Finally, the report highlighted the importance of **understanding the data** before creating a report. By exploring and understanding the metrics in the data set, it became easier to identify important correlations, trends, and insights that could be used to draw meaningful conclusions. The countries with the highest life expectancy were Australia, Singapore, Switzerland and Hong Kong, while the countries with the highest GDP per person were Singapore, Macau, and Monaco. In 2019, the United States had a life expectancy of 79.1 and a GDP per person of $62,530. Other countries such as United Arab Emirates, Brunei and Kuwait had a lower life expectancy and GDP per person. There are different factors that contribute to life expectancy and GDP, such as access to healthcare, education, and economic systems. Governments should consider policies that can be implemented to improve life expectancy and GDP in countries with lower values.

In conclusion, creating a Tableau report about the top 20 countries by GDP per person revealed several important insights about the economic standing of each country and the correlations between them. Additionally, the process highlighted the importance of understanding the data before creating a report.

Dig Deeper

 Each visualization is displayed using the same report space (size of the background).  
  
🔹 Despite of the fact that presented individual visuals in Dashboard 1 and 2are created using the same space, they display data in a different way. Visuals usually offer slightly different formatting options, which can either enhance or limit the overall transparency.  
  
🔹 Some important aspects to consider when selecting visuals (amongst some others):  
  
◻️ visual performance (time loading, table might take more time to load because of greater amount of used measures)  
  
◻️ # of data (metrics) displayed on a single visual (i.e. following bar chart or waterfall chart display GDP per capita as USD whereas pie chart or a table may additionally display % structure; some visuals provides additional information regarding the total value, others not)  
  
◻️ 'effectiveness' of given visual (i.e. multi-cards do not show scale, whereas tree map presents scale but in less transparent way comparing to i.e. data bars). Some visuals provides more formatting options (i.e. conditional formatting, that can enhance data-storytelling)

Here are some of the main similarities and differences between GDPR and DPA 2018:

Similarities:

* Both GDPR and DPA 2018 aim to protect the privacy and rights of individuals with respect to their personal data.
* Both GDPR and DPA 2018 require organisations to obtain valid consent from individuals before collecting, using, or processing their personal data.
* Both GDPR and DPA 2018 provide individuals with the right to access their personal data, to correct or delete it, and to object to its processing in certain circumstances.
* Both GDPR and DPA 2018 impose strict requirements on organisations to ensure the security of personal data and to report data breaches to the relevant authorities and affected individuals.

Differences:

* GDPR is a regulation that applies to all EU member states and has extra-territorial effect, while DPA 2018 is an act that applies only to the UK.
* GDPR has higher penalties for non-compliance, with fines of up to €20 million or 4% of an organisation's global annual turnover, whichever is higher, while DPA 2018 has maximum fines of up to £17.5 million or 4% of an organisation's global annual turnover, whichever is higher.
* GDPR provides more extensive rights for individuals, such as the right to data portability and the right to be forgotten, which are not included in DPA 2018.
* DPA 2018 includes some additional provisions that are not covered by GDPR, such as exemptions for certain types of data processing for specific purposes, such as journalism, research, and archiving.

Overall, while there are some similarities between GDPR and DPA 2018, organisations that operate in both the EU and the UK should ensure they are compliant with the specific requirements of each regulation to avoid any potential legal or financial penalties.