Does your analytics platform facilitate or obstruct your ability to comply with GDPR?

If you are using a BI software stack - databases, ETL, analytics, and visualizations - you need to review how you are storing and processing your data. The European Union's General Data Protection Regulation (GDPR) has stringent requirements on personal data protection, traceable data movement, and secure data access. You are responsible as a data controller or processor to ensure all your processes, systems, and platforms comply with the GDPR around personally identifiable data. And your data analytics platform is one of the critical platforms you need to assess.

Be GDPR ready: Choose a data analytics platform that helps you to comply

We, as a data analytics platform vendor, understand the stresses that the GDPR can bring when you consider your data analytics on personal data. So, we want to help alleviate some of those stresses by providing a short guide to some of the requirements you face under the GDPR and the ways your analytics platform can help, or hinder, your compliance.

At Yellowfin, we want to help you comply with the GDPR. Yellowfin is one of the world's leading Business Intelligence (BI) and analytics platforms. It's built with data governance and security in mind. It does not store your data in a proprietary database or engine, so you don't create multiple copies of your data and your data always remains yours. Yellowfin is one, integrated platform. Its centralised design, accessed through a web portal, prevents the creation of data silos, provides transparency, and prevents the copying of data to a desktop. You can analyse your data in one place and implement comprehensive security and governance features with ease.

Your data requirements under GDPR

The requirements of the GDPR are vast and often daunting. But there are a few key principles you must address when considering the role of your data analytics tool in analysing data that falls under the new legislation. Listed below are some of the key requirements you need to meet under the GDPR:

1. The ability to track the use and movement of personal data across the business.
2. Data and IT security.
3. Make sure the data you hold and use is only kept for the purposes that were consented to, or for purposes that come under legitimate interest.
4. The ability to provide the supervisory authorities with documentation on how the company tracks and controls personal data across all the business platforms and systems.
5. The ability to comply with the 'right to be forgotten' that allows an individual to request all their data to be removed from your systems and platforms, fast.

The GDPR laws apply to the use of data that enables an individual to be identified, which includes names, email or physical addresses (including IP addresses), ID numbers etc. This means you can continue to analyse your general business data as before, but the processing or profiling of any data that concerns an individual and makes them identifiable must comply with the GDPR.

Privacy by Design

Unfortunately, many data analytics platform hinder rather than help your compliance with the GDPR. They obstruct your ability to design processes as described in the GDPR principle of Privacy by Design. Desktop versions of analytic tools prevent centralised data governance, and workbook-style tools allow individuals to easily copy data onto their device. You lose the ability to trace the data's journey and monitor its use. How will you know if there has been a data breach if you don't know all the places the data is stored? How can you facilitate the monitoring of data use according to consent, or trace the data's final destinations to delete it if required under 'the right to be forgotten'?

By using Yellowfin, which has been built with governance and security in mind from the ground up, you are able to implement and demonstrate compliance with GDPR requirements on your data analytics platform. If you use Yellowfin, you can know that your front-end analytics meets the 'privacy by design' approach because it simply reports off your data source. Yellowfin also provides centralised governance and control of the analytics.

Here is how your analytics platform should, and Yellowfin does, help you comply with some of the main GDPR requirements.

1. Track all personal data across the entire company

It's a huge task, especially when so many businesses have multiple databases and software systems across departments and data silos that prevent transparency. You will need to implement Privacy Impact Assessments (PIAs) to map out user stories for what data you hold, where it came from, who you share it with, and what you do with it. You need to also consider the processes around how you collect, store, and process the data you hold.

Yellowfin helps you track data analyses by providing a data lineage to track your data from source to where it is distributed.

Yellowfin does not store your raw data

Yellowfin does not store your raw data, it simply reports off it. Your data stays in your databases, data sources, and data warehouses. This is a big advantage of using Yellowfin over BI solutions that often lock you into their proprietary databases and so store your data. Yellowfin has no access to any of your data. Yellowfin queries your data sources directly and does not

force you to move data into a proprietary store or engine through which someone could gain access to your data. So, the governance you place on your data at the point of storage remains unaffected. And, if the driver you use to connect to your data source from Yellowfin allows, you can configure encryption on the connection to your data.

There are no desktop versions of Yellowfin in which people can create their own copies of the data. This contrasts with many other platforms where the data is stored in proprietary databases and engines and copies of data can be made in the workbook and sheet file structure.

Internal training for analytics compliance

The reports that you create from the data, in which an individual could be identified, must comply with the GDPR. This requires internal training for data analysts and other data controllers and processors on what data can be used and how under the GDPR laws of 'consent' and 'legitimate interest'. Once educated, the data analysts and platform users can utilise the platform's security and governance capabilities to minimise the risks of internal data breaches and data misuse. Yellowfin provides detailed documentation and consultancy options to help you implement its comprehensive security and governance capabilities effectively.

Know who has created and looked at which reports

Within Yellowfin, administrators can use the audit log, which displays an events table. This shows which data sets were added or used to create reports and who created them. It also shows who accessed those reports. The log can be configured to display events for a set period into the past, and those events will then be archived. Make sure that, whichever platform you use, you are able to trace the data's journey.

Having an events log gives you a comprehensive view of who saw what data in order to trace the usage of the data in analyses. This helps you trace whether the personal data has been analysed in line with consent given or legitimate interests identified. It also provides a means of tracing any internal data breaches back to the source, and make sure that only people with the correct permissions are creating and viewing reports. This also helps with tracing where personal data has been analysed to enact the right to be forgotten, if requested.

2. Security - ensure only the right people have access to sensitive data

> *"Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."*
>
> **- ICO, Principle 7**

You need to have appropriate security in place to prevent personal data being compromised. This includes ensuring only authorised people can access, alter, disclose or destroy personal data. It also means that if any personal data is accidentally lost, removed, or altered, it needs to be able to be recovered. Yellowfin has been built with security at its core, so those viewing reports cannot accidentally lose, remove or alter data at the source using Yellowfin.

Data access restrictions and permissions

For access authentication, Yellowfin has two methods configurable from the Admin Console – Yellowfin Authentication, or LDAP Authentication. Yellowfin Authentication means that the user's credentials (user ID and password) are stored and encrypted in Yellowfin and checked to authenticate a user logging into the system. LDAP Authentication means that Yellowfin references an external directory (LDAP) or database to perform the authentication - a user will enter their user ID and password (or this will be passed by Single Sign On) and Yellowfin will authenticate these details with those in the LDAP directory. Any removal or lockout of the user in the LDAP directly will automatically flow through to Yellowfin.

But the security doesn't stop there. Yellowfin's access filters allow you to make data visible only to those who have permission so sensitive data does not get into the wrong hands. You can implement content level security for individual reports and dashboards, and even put row level security in place using source filters. In addition, you can define which users have the rights to create views against a data source as well as write SQL queries against the source. Views, and even specific columns within a view, can have access restrictions implemented too.

Authorisation processes for data reporting

Yellowfin also has an inbuilt approval workflow to ensure the reports and dashboards go through a checking process before being released to the business. Approved content carries a watermark. This gives you confidence in the trustworthiness of the data analysis and the report only gets released once it is approved for the audience.

Mobile device security

Another concern for businesses under GDPR is the security of data access through mobile devices. Yellowfin has Android and iOS apps available. All the same governance and security of Yellowfin applies to mobile. In addition, if a mobile device is lost or stolen, Yellowfin allows you to disable the mobile application centrally so nobody else can access your reports through the missing device.

3. Consent and legitimate interest

Personal data may only be used for clear and legitimate purposes under the GDPR. If the data is to be used for a purpose other than the one for which it was originally collected, additional consent must be gathered from the individuals concerned. However, some data processing falls into the category of 'legitimate interests'. This applies when you use people's data in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing. Yellowfin helps you trace how data is being used in analysis.

Data lineage - trace where data came from and who used it

As explained already, Yellowfin has an events log that gives oversight of which data sources have been added and who has used them and viewed the reports. This gives a data protection officer the reassurance and the tools they need to help them keep record that personal data has been used in compliance with the GDPR and the consent given at the point of collection.

Our data transformation flows can mask sensitive data

> *The DPA does not prohibit the disclosure of personal data, but any disclosure has to be fair, lawful and in compliance with the other data protection principles.*
>
> **- ICO, 'Anonymisation: managing data protection risk code of practice'**

If you wish to analyse personally identifiable information, you can opt to anonymise sensitive data. Yellowfin enables you to do this in Data Transformation. The module allows a technically-able person to use masking advanced functions or write a script that can be used as a transformation step.

Be aware that, although an individual may not be able to be identified using the anonymised data alone, an individual's identity may be able to be inferred when external data is used in combination with the data you hold. Wherever possible, you must mitigate and minimise the risk of an individual being identified through the data using sensible judgement.

4. Providing authorities with documentation

A further requirement under the GDPR is the need to maintain a record of processing activities under your business' responsibility. This is best achieved by first undertaking an information audit or data-mapping exercise. This will shed light on what personal data your organisation holds, where it is, and how long you hold it for. You then need to ensure that the data is processed within the bounds of the GDPR by you and by any third-party processors you use. If you use third-party processors, you will need contracts with them that ensure they only process data as directed by you within the bounds of the GDPR.

If you process data using Yellowfin, you can rest assured that we as a company have no access to the data you analyse within the platform. This removes the need for a third-party data processing agreement with us because we don't hold or process your data. As stated in our End User License Agreement (EULA), you maintain full control and responsibility for your own data and processing activities.

5. EU citizens have the right to be "forgotten"

Companies must also demonstrate that they can remove any instance of personal data from all systems and platforms at the request of the person concerned (if their request falls within the allowances of Article 17 of the GDPR).

When it comes to deleting reports that contain analyses of that person's data, Yellowfin allows you to easily delete individual reports and dashboards. Even better, if you remove the data at the data source, Yellowfin will reflect that change on the next scheduled report or dashboard refresh because the data is reported directly from the data source - there is no intermediate proprietary database holding stage. You can easily run a manual refresh if the scheduled update falls outside of the timeframe in which you need to remove the data.

Data analytics and GDPR compliance - is your tool helping?

When it comes to auditing, documenting, tracking, and validating the data you hold on individuals, the task is anything but easy. And too many data analytics and BI tools only add to the headache. Ungoverned and untraceable data and analyses created on desktop solutions create a security nightmare. Workbook-style tools mean duplicates of your data can be created - a huge governance flaw. And solutions that lock you into proprietary databases and engines mean that your data is held by a third party, which requires you to scrutinise them further for security and ensure all the correct agreements and documentation is in place.

But your data analytics platform doesn't have to give you these huge GDPR headaches.

Yellowfin does not store or process your data; we are serious about security; and we facilitate your compliance with GDPR. Yellowfin offers you a single, centralised platform that allows you to closely govern your data and the analytics of that data. No desktop versions. No workbooks. No proprietary databases and engines. The Yellowfin platform simply reports directly from your data source. And Yellowfin, the company, cannot see your data.

We want to help you, not hinder you, in complying with GDPR. Take time to consider just how easy it is to align your data controlling and processing with GDPR with the analytics platform you currently use. If you need to upgrade to a centralised platform that helps you govern and secure your data and analytics, Yellowfin might just be the answer. We facilitate privacy by design.

Yellowfin provides a Business Intelligence (BI) and analytics platform aimed at solving real enterprise analytics challenges and helping business people understand not only what happened, but why. Founded in 2003 in response to the complexity and costs associated with implementing and using traditional BI tools, Yellowfin is an intuitive, 100 percent web-based reporting and analytics platform. More than 25,000 organisations and more than three million end users across 75 countries use Yellowfin every day.

For more information, visit
www.yellowfinbi.com