GDPR+Cognisess

Cognisess aims to democratise human capital; empowering every individual and every organisation to understand and enhance their talent and potential.

Collecting, processing, storing, and safeguarding your data with an emphasis on security and privacy is a key part of creating a trustworthy and reliable system.

Introduction

The use of online platforms for recruitment and performance management is a complex process that can result in the collection of a lot of sensitive data. Collecting, processing, storing, and safeguarding this data with an emphasis on security and privacy is a key part of creating a trustworthy and reliable system. As a leader in predictive people analytics, Cognisess is experienced in handling data for organisations of all sizes, across the globe. We believe privacy is a fundamental right and that regulation is an important step forward in protecting and enabling the privacy rights of individuals.

The intention of this document is to better inform our clients about the General Data Protection Regulation (GDPR), the global standard for data privacy rights, and to share our suggestions and experiences with collecting, storing, and using data in a compliant manner. Please note that this document is not intended as legal guidance and that issues will be discussed in general terms. If any questions arise, or if you would like more information about specific use cases, please get in touch with us.

Who is affected by GDPR?

GDPR applies to the processing of anyone's personal data, if the processing is done for an organisation established in the EU (regardless of where the processing takes place), such as in the case of Cognisess. It also applies more generally to the processing of personal data of EU residents by an organisation established outside the EU, where that processing relates to the offering of goods or services to those individuals or to the monitoring of their behaviour.

Since Cognisess believes in the empowerment of its users to make the most of their rights under GDPR, we recognise the rights GDPR gives to users regardless of their location. Our mission to uphold fairness in the hiring process extends to all facets of the process, including our commitment to data protection and privacy.

The Seven Key Principles

There are seven key GPPR principles that organisations must comply with:

Principle 1: Lawfulness, Fairness, and Transparency

Under this first principle, data collectors need to be clear with individuals about how personal data is being used and they also need a "lawful basis" to process that data. There are six lawful bases that may be used to justify data collection and processing. Cognisess cites the following three bases: Consent from the data subject, legal/contractual obligation, and the legitimate interests of an institution/business. As for our transparency, users are informed about their data rights and usage throughout the platform and in our **Data Protection Policy**.

Principle 2: Purpose Limitation

The processing of personal data should be limited to specified, explicit, and legitimate purposes. Personal data cannot be re-used or disclosed for purposes that are not "compatible" with the purpose for which the data was originally collected; these compatible purposes include scientific research and statistical processes. Cognisess collects user data to help identify the best candidates for a job and we do not use that data for any other purposes beyond the scope of our platform, and research for improving the platform.

Principle 3: Data Minimisation

GDPR states that the collection and storage of personal data should be minimised to that which is adequate and relevant for the intended purpose. For Cognisess, that means we only collect data that we know has a bearing on assessing a candidate's suitability for a role, nothing more, nothing less.

All of the assessments that we provide on the Cognisess platform have undergone rigorous testing during their development and are assessed for their reliability and validity on a regular basis. Rest assured that the data we collect from assessments is relevant for the areas that they are designed for.

We can also minimise data collection by implementing a multi-staged assessment structure. By assessing candidates and their skills in multiple steps, only the candidates that best fit the role will move on to further assessments. This significantly reduces the amount of unused data that gets collected. Waste not, want not.

Principle 4: Accuracy

Responsibility for inputting accurate personal data lies with the individual but they must be able to correct or request the deletion of their data at any time. These changes can be made by editing a user's profile page or requesting a deletion from the 'Manage my account' menu option.

Principle 5: Storage Limitation

Companies cannot keep personal data indefinitely. Personal data can only be retained for as long as necessary to achieve the purposes for which the data

was collected. To comply, Cognisess will delete any personally identifiable information relating to accounts that have been inactive for over two years.

Principle 6: Integrity and Confidentiality (Security)

Data is one of the most important resources that can be used and stored by a company, and at Cognisess we work hard to protect and maximise the data we collect on your behalf. We know some organisations and users are still wary of the cloud. Keeping data confidential is essential for any company, and that is why Cognisess uses Microsoft Azure as its cloud computing platform to host our applications and your data.

Microsoft has made an industry-leading commitment to the protection and privacy of your data. They were the first cloud provider recognised by the European Union's data protection authorities for its commitment to rigorous EU privacy laws. Microsoft was also the first major cloud provider to adopt the new international cloud privacy standard, ISO 27018. Azure meets a broad set of international, industry-specific, and country specific compliance standards.

Data is a valuable and irreplaceable asset, and encryption serves as the last and strongest line of defence in a multi-layered data security strategy. Cognisess takes advantage of Microsoft Azure's encryption technology to safeguard data and help maintain control over it.

Encryption transforms data so that only someone with the decryption key can access it. Azure uses industry-standard, secure transport protocols for data as it moves through a network—whether between user devices and Microsoft data centres or within data centres themselves. Hence, we can guarantee that the data used by Cognisess is as safe throughout its entire life cycle as state-of-the-art technology permits.

Cognisess constantly monitors its systems to prevent security breaches. We implement security safeguards designed to protect your data, such as HTTPS. Through these measures, we endeavour to keep even the smallest pieces of data safe and secure. Any attempt to breach the servers running our platform or hosting our databases will result in immediate notification to Microsoft security specialists as well as to our internal specialists. By doing this, we ensure that any attempt to obtain private data will be dealt with extremely quickly by a dedicated professional.

Principle 7: Accountability

The final principle, accountability, requires that companies take responsibility for the proper use of personal data and compliance with the other GDPR principles. This includes having procedures for compliance in place and appropriate records to demonstrate those preparations. This document, among other, internal documents, serves as an example of our commitment to compliance.

Common Misconception #1:

Paper-based is compliant

Many of our clients and partners have asked us how using Cognisess could be more compliant than sticking to old paper-based approaches, but GDPR applies to all personal data regardless of how it is stored. This means that for many of our clients, our online and fully digital systems are compliant with GDPR whereas their previous paper-and-pencil versions or local digital data storages (such as spreadsheets on a computer) were not compliant.

Cognisess is a cloud-based service which means that our data is stored on highly secure Microsoft Azure servers. This also allows us to handle data in its country of origin, as mandated by some countries' data protection legislation.

Common Misconception #2:

You need to be a large company to be affected by GDPR and to be compliant

GDPR applies more broadly than might be apparent at first glance. Unlike privacy laws in some other jurisdictions, GDPR is applicable to organisations of all sizes, in all industries.

We are very proud to work with some of the largest companies in their respective fields and industries, such as the world's largest beer brewer. With these clients, we went through extensive preparations before the launch of GDPR to ensure that their data is handled, processed, and stored in a fully compliant and secure way.

The benefit of using the Cognisess platform is that all clients – regardless of company size – now benefit from the data handling and processing architecture that ensures data compliance for our global enterprise partners.

It is still very important for us to understand how you collect data, where it comes from, and how it should be processed – so please feel free to get in touch with the accounts team to help us set up the right parameters on the platform for your needs.

Common Misconception #3:

You need to be both an HR and data expert to be able to use predictive analytics in a compliant manner

It is of course always good to have specialists at your disposal to cover these areas in detail, but we understand that not all of our clients have this expertise in-house. This is why we provide both the knowledge of how to make the most of the data you already have and will collect with our tools, and the assurance of GDPR compliance.

With Cognisess, you can be confident in the science and data protection behind the platform, giving you more time to focus on your job candidates and the skills they can bring to your company. We make the analysis easy and approachable for all technical skill levels.

International Compliance

The EU is often viewed as a role model on privacy issues internationally, so we also expect to see concepts from GDPR adopted in other parts of the world over time. Since all of the data we collect on our platform is stored on Microsoft Azure's secure servers, we can ensure that our encryption is of the highest industry standard at an international level, and it is constantly updated by industry experts.

Because Azure meets the strict regulations for data storage across the European Union as well as other international standards, Cognisess can host data across a wide range of nations. This is often a very important requirement for specific national standards. By meeting these standards, Cognisess can proudly offer services to a wide range of businesses across the globe.

Platform Tenancy

The platform is multi-tenanted with distinct organisational sign-ins. With localised servers, it is possible to create a single-tenant instance of the platform, or to use an instance shared with fewer other organisations if it is a key requirement for deployment. This would be at an additional cost for the server localisation/bespoke deployment of a production instance of the platform.

Sensitive Data

When considering sensitive user information, we are aware that it is necessary to give assessment and profiler results without compromising the confidentiality we owe to those who use our system. Therefore, when giving an overview of personality, we only ever display a summary of a user's general personality traits, without giving out the responses to specific questions. By doing this we can share the information that an employer would need, whilst simultaneously keeping quite personal data confidential. To run a completely 'blind' recruitment process, admins can choose to anonymise users from the very start, making their identity untraceable even by Cognisess.

Data collected for employee engagement and other staff surveys is aggregated and released as group data, meaning that if a certain threshold of minimum user completions has not been met, the platform will lock the results. This ensures that no user is identifiable when completing anonymous surveys. The normal release groups are 5 or 10 completed responses.

Administrator profiles with access to these results are always attached to a specific individual with password protection, and the data is still encrypted to the highest standard, ensuring that all data is safe for both user and manager.

Data Protection Officer

If you have questions regarding our policies or your data, please contact our Data Protection Officer by email: **dataprotection@cognisess.com**

Data Protection Officer

If you have questions regarding our policies or your data, please contact our Data Protection Officer by email:

dataprotection@cognisess.com

Head Office

Cognisess Ltd 10 Argyle Street Bath BA2 4BQ
United Kingdom

Partner Locations

China, Singapore, USA, UK, The Netherlands, Australia, Israel, South Africa

02/02/2021

For more information about how we can help your organisation, please get in touch on: **support@cognisess.com**