DATA PROTECTION+Cognisess

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

We believe that your right to data protection is fundamental, so users regardless of their location will benefit from the data subject rights set out in the EU's General Data Protection Regulation (GDPR).

Your Data Protection Rights

We believe that your right to data protection is fundamental, so users regardless of their location will benefit from the data subject rights set out in the EU's General Data Protection Regulation (GDPR). These rights include the right to be informed, the right of access, the right to rectification, the right to erasure, the right to restrict processing, the right to data portability, the right to object and rights related to automated decision making, including profiling. This document will detail how Cognisess works to ensure these rights are not only upheld but highlighted and made accessible for its users.

GDPR in Brief

The data subject rights outlined below come from GDPR legislation. The main tenets of GDPR that data collectors must abide by are lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, confidentiality, and accountability. More information about how Cognisess meets these standards can be found in our **GDPR statement**.

Transparency + the Right to be Informed

In order to be able to make the data decisions that best serve your interests, first you need to know how Cognisess collects and uses your personal data. We collect only the data that you provide us with, whether that be from filling out surveys, playing assessments, or uploading your CV or interview videos. Cognisess does not scrape data from the Internet to learn more about our candidates as we find that is neither a fair nor high quality source of information.

All of the information that we collect is optional to provide, but by sharing details like your gender, ethnicity, or disability status, we can better identify and eliminate bias. Users can remain completely anonymous throughout the hiring process if they so choose. Users signing up as employees of an organisation will have to provide a little more information in order for us to do the appropriate benchmarking and analyses. However, employee data will not be used for other purposes unless we receive permission from these users.

Data is never sold to or shared with third parties without your consent.

The data processing we do includes collecting assessment scores, the calculation of job profiler scores, the calculation of inferred variables and attribute values, and the work of the AI models that comprise our video analytics tool. We do not fully automate any hiring campaign, so there will

always be a human making the decision about who moves onto the next stage of hiring.

Exploring your Results + the Right to Access

Users have the right to access all of their data that is stored by Cognisess. Typically, this information must be retrieved by making a subject access request, but Cognisess makes this simple by letting all users see the results of their assessments. We will never keep your assessment scores from you, and you have access to view your profile and scores at any time by logging into your account. There, all of your assessment, attribute, and Q Scores can be found alongside personalised summary reports on your performance.

Editing your Profile + the Right to Rectification

To ensure that all of your data is correct and up to date, Cognisess users can update their profile, adding new information or changing any of the personal information previously entered. This includes your name, title, disability status, gender, ethnicity, and the CV content such as education history and language ability. This way, you can always be sure that we have the latest, correct version of this data. We have no limits on how often or when you can change this information, so changes can be made on your schedule, no assistance from the Cognisess team needed.

Closing your Account + the Right to Erasure

The right to erasure, also known as 'the right to be forgotten', means that you can close your account with us at any time. This can be done by going to your profile page by clicking on the ••• menu in the profile banner and selecting the 'Manage your account' option. Closed accounts will have their personal identifying information deleted while assessment scores are kept in an anonymised format for score norming purposes. This anonymisation for norm groups is a GDPR-approved reason for Cognisess to retain information after an account closure. These scores are kept in such a way that they cannot be connected back to you or your former account. Account closures will take a brief amount of time to be reflected in both our servers and backups but is permanent once begun. Any account that has been inactive for over 2 years will also be subject to account deletion.

Hitting Pause + the Right to Restrict Processing

The right to restrict processing gives users the ability to request that a company pauses the collection and use of their data for a finite period of time. This right only applies in a few cases, the most common and applicable being the case that a user wishes to contest the accuracy of their personal data. Since users can change the personal information they have entered in their profile at any time, this right would only apply if a user wishes to contest the accuracy of the assessment or job profiler scoring process. We welcome questions about our processes, but users can be confident in our science-driven approach built by psychologists, neuroscientists, and data scientists. If a user still wishes to exercise their right to restrict processing, they should get in touch with our Data Protection Officer: **dataprotection@cognisess.com**

Downloading your Results + the Right to Data Portability

Users who wish to receive a machine-readable copy of their Cognisess data and results can do so via their right to data portability. This is quite similar to the right of access which allows users to view their results, but data portability lets users receive their data in a format such as a CSV, XML, or JSON file which can easily be read and processed by a computer. Such requests can be made by contacting our Data Protection Officer, and they will be fulfilled within one month as mandated by GDPR.

Withdrawing Consent + the Right to Object

If a user no longer wishes to have their data processed by Cognisess, they can either choose to close their account, or cease to input new data into the platform (take no further assessments or add no further profile details). However, if a user does not delete their account, this does not keep data from being visible to organisational administrators and Cognisess team members. Since the right to object does not apply in all situations, it may not be the best option for your needs. Our Data Protection Officer can better cater our solutions to your specific case.

Ethical AI + Rights Related to Automated Decision Making

Under GDPR, individuals cannot be subjected to automated decision making that does not involve any human controls on the system. While Cognisess does use AI products to assist the decisions being made by HR professionals, we will never automate these processes completely. When decision making is fully automated, users have the right to be informed about how the processing works, must be given the ability to easily request human intervention or to challenge the decision, and the system must be checked regularly to ensure it is working properly.

Even though our decision making systems are not fully automated, we will strive to provide users with comprehensive information about how these systems work and how they are maintained, and we encourage users to raise concerns or challenges. Ethical AI is about transparency, trust, and collaboration between the data subjects and the data processors. Further information about our ethical use of AI can be found in our **Ethical AI statement**.

Reaching out + the Right to Raise Concerns

If you have any concerns about your data's safety or how we are processing your data, please reach out to our Data Protection Officer. Otherwise, all data subjects have the right to make a complaint to the Information Commissioner's Office (ICO) if they feel their rights are being violated.

Direct Marketing

Cognisess will never sell advertising alongside your account. You have the option to opt out of our marketing emails and you always can always unsubscribe.

Data Storage Locations

All of our data is hosted on Microsoft Azure servers, which allows us to host data in a specific country, as some national data protection legislations require. We currently operate servers in the UK, Europe, Australia, and China. While data can be moved between these servers, such action would only be taken at an organisation's request and in accordance with local data protection law.

Data Privacy

We at Cognisess understand the private and sensitive nature of the data you entrust us with. Whether it is your job history from your CV, your answers to our LensPro personality assessment, or information about a disclosed disability, Cognisess aims to not only protect your data, but to also treat it with respect. The data that you enter on the platform has varying levels of visibility to different types of users.

Other candidates or employees cannot access any information about other candidates or employees on the platform. While these users can see all of their own data, that is the only data they can access. Organisational administrators, such as HR managers, can see data for their team members, employees, and candidates within their organisation. There are still limits on the information that they can see about each of these types of users. Administrators can see scoring and assessment information, the contents of a user's profile, and comparisons of these factors across users. However, information like individual answers to the LensPro personality assessment, user details on anonymised surveys, and disabilities that have not explicitly been marked as to be shared with employers cannot be accessed by these administrators.

Internally at Cognisess, the development team, the research and development team, the support team, as well as account managers have access to user and organisational data in order to provide services that relate to users and organisations. This data is accessed on secured, dedicated machines, and the Cognisess team members have all signed agreements that we will not share or disclose the private information and data of our platform users. Your privacy and trust in us are of the upmost importance to the team. We use measures like anonymising users and storing passwords in 'hashed' and 'salted' formats to safely store information in our database, meaning even members of the Cognisess team cannot view your password.

No external parties are granted access to the data unless it is legally required for us to provide access (e.g. by court order). No data is ever sold, shared, or in any other way distributed or made accessible to third parties.

Security Measures

All Cognisess data is stored and processed on Microsoft Azure servers. This means that it is encrypted at rest and is protected by the Microsoft Firewall and constant attack/breach monitoring. Offline activities and data modelling are carried out on dedicated and secured machines. If, despite our best efforts the privacy and security of our users' data is compromised, Cognisess will, in accordance with GDPR, notify the affected users of the breach.

We work hard to make our system and the use of it as safe and reliable as possible. To ensure this, we need your help. We suggest taking a few measures on the user-end to help keep the platform secure.

- **Passwords should be individual, hard to guess, and contain mixtures of numbers, letters and, ideally, symbols. It is easy to retrieve a lost password in case you forget it, so please make it as secure as you can.**
- **Do not share your account details with anyone. Cognisess support staff might ask you for your name, username, or email address to find you on the system, but we never need your password. Please do not share it with anyone.**
- **Please ensure that you are using a secure and encrypted Internet connection. Public networks or non-encrypted shared networks are generally not advisable for sending and receiving confidential information.**
- **Please be sure to log off of the platform fully once you are done, and do not leave your computer unattended while logged in.**

Users are responsible for keeping their log-in details secure and to inform the organisation or Cognisess directly of any existing or suspected instances that might compromise their account security.

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

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