POLICY DETAILS	
Policy Name:	DPS-05 Privacy Policy / Notice
Purpose & Context:	To explain how your personal data is collected, used and protected, ensuring transparency and your rights under data protection law.
Applicable Company:	Cognacity Health Ltd and Cognacity Ltd (Cognacity)
Scope:	This policy applies to all clients, corporate clients and any individuals who use our services.
Public or Private Facing:	Public

1. INTRODUCTION

This Privacy Policy / Notice outlines the principles and commitments of Cognacity. We are dedicated to respecting your privacy and are committed to protecting your personal data. This Privacy Notice will inform you as to how we look after your personal data and tell you about your privacy rights and how the law protects you.

2. SCOPE & APPLICABILITY

This Privacy Notice gives you information on how we collect and process your personal data when you engage us to provide you with services. By 'services' we mean our clinical, coaching, leadership assessments, advisory and workshop services which are explained more fully on our website (www.cognacity.co.uk).

It is important that you read this Privacy Notice when we are collecting or processing personal data about you so that you are fully aware of how and why we are using your data.

3. CONTROLLER

The controller of your personal data will be one of three entities, depending on which service you engage us to provide:

3.1. If you are engaging us for the provision of clinical services ('Clinical Services'), i.e. for the treatment of any mental health condition by members of our team of psychiatrists, psychologists and/or psychotherapists, the controller responsible for your personal data is Cognacity Health Limited, a company registered in England and Wales under registration number 13866879.

3.2. If you are engaging us for the provision of coaching services and/or psychometric assessments and/or workshop/webinar delivery ('Non-Clinical Services'), the controller responsible for your personal data is Cognacity Limited, a private limited company incorporated in England and Wales under company number 07431120.

3.3. If you are a corporate client engaging us for the provision of Leadership Assessments, you will be the controller responsible for the personal data of the candidates we assess and Cognacity Ltd will be the processor. Where you are an individual being assessed under such an engagement,

your personal data is controlled by the engaging organisation, not by Cognacity, and this Privacy Notice should be read alongside the privacy notice provided to you by that organisation.

3.4 If you are being referred to us by your employer for an independent Occupational Health Assessment, the controller responsible for your personal data is Cognacity Health Limited.

Cognacity Ltd and Cognacity Health Ltd both have their registered office at 22 Welbeck Street, London W1G 8EF. Cognacity Health Ltd is the parent company and collectively they are referred to as "Cognacity", "we", "us" and "our" in this privacy notice. Both entities are registered on the data protection public register: Cognacity Health Limited under registration number: ZB425974 and Cognacity Limited registration under registration number ZA392828.

Cognacity Health Ltd operates under a different set of regulatory requirements than Cognacity Ltd.

If you have any questions about this Privacy Notice, including any requests to exercise your legal rights, please contact our Data Protection Officer by emailing privacy@cognacity.co.uk.

You have the right to make a complaint at any time to the Information Commissioner's Office, the UK supervisory authority for data protection issues (www.ico.org.uk). We would, however, appreciate the chance to deal with your concerns before you approach the ICO so please contact privacy@cognacity.co.uk in the first instance.

4. YOUR DUTY TO INFORM US OF CHANGE

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your relationship with us.

5. THIRD PARTY LINKS

Our website may include links to third-party websites, plug-ins and applications. Clicking on those links, or enabling those connections, may allow third parties to collect or share data about you. We do not control these third-party websites and are not responsible for their privacy statements. When you leave our website, we encourage you to read the Privacy Notice of every website you visit.

We may, as part of our Non-Clinical Services, ask you to complete a psychometric test. This may be (i) as part of our leadership assessment services: or (ii) via our own online platform which we make available at www.cognacity.digital. The differences between the two are set out below:

5.1. Our leadership assessment services: Our leadership assessment service uses third-party psychometric tools which require your explicit consent for data processing by those third parties. In this context, Cognacity acts as the data processor while the company that engages us to conduct the assessments serves as the data controller. The results of your psychometric assessments are evaluated by Cognacity and fed back to the instructing company.

5.2. Our on-line platform: Cognacity's online platform is operated by Cognacity Limited which (as with the other services we provide) is the data controller in respect of any personal data you submit via this platform. Our lawful bases of processing personal data via this platform are set

out in the table below, but please note that personal data you submit through the platform is not shared with your employer or any third party. We may anonymise personal data and – aggregated across a significantly sized group level – feed it back to your employer in the form of reports about the general wellbeing of employees within your organisation. The size of the cohort is such that no individual will be identifiable from this data. You do not have to complete the psychometric test if you do not want to (and there are no negative consequences in not completing it). The questions contained within the psychometrics all relate to the status of your mental wellbeing/resilience-levels and provide an overview of your mental health and help identify those individuals who may require additional support.

6. THE DATA WE COLLECT ABOUT YOU

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

We may collect, use, store and transfer different kinds of personal data about you which we have grouped together as follows:

6.1. **Identity Data** - includes your first name, maiden name, last name, marital status, title, date of birth and gender.

6.2. **Contact Data** – includes your home and/or work address, your personal and/or work email addresses, telephone numbers and emergency contact details.

6.3. **Financial Data** – includes your bank account details and payment card details.

6.4. **Transaction Data** – includes details about payments to and from you and other details of services we have delivered.

6.5. **Technical Data** – includes your internet protocol (IP) address, browser type and version, time Zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices you use to access our website.

6.6. **Profile Data** – includes your interests, preferences, feedback and survey responses.

6.7. **Usage Data** – includes information about how you use our website and services.

6.8. **Marketing and Communications Data** – includes your preferences in receiving marketing from us and our third parties and your communication preferences.

6.9. **Health Data** – includes any information relating to your health that you, or a third party on your behalf, provides to us. Health Data is sensitive personal data to which UK GDPR applies special rules.

Where we need to collect personal data by law, or under the terms of a contract we have with you or your sponsor and you fail to provide that data when requested, we may not be able to perform the contract we have or are trying to enter into with you (for example to provide you with our services). In that case, we may have to cancel the provision of services to you but we will notify

you if that is the case at the time.

7. HOW IS YOUR PERSONAL DATA COLLECTED?

We use different methods to collect data from and about you including through direct interactions. You may give us your Identity Data, Contact Data, Financial Data, Profile Data, Marketing and Communications Data and Health Data in person at our clinic or by corresponding with us by post, phone, email, filling in forms on our website, accessing online portals or otherwise. This includes personal data you provide when you:

7.1. instruct us to provide you with any of the services we offer;

7.2. provide us with information in order to allow us to provide you with our services or otherwise fulfil our obligations pursuant to any contract we have with you;

7.3. subscribe to any publications or information on our website;

7.4. request marketing to be sent to you;

7.5. respond to any survey we provide to you; or

7.6. give us any feedback.

8. HOW WE USE YOUR PERSONAL DATA

When we will use your personal data (pursuant to Article 6 of the UK GDPR)

We will only use your personal data when the law allows us to. Most commonly, we will use your personal data in the following circumstances:

8.1. Where you have explicitly consented to our use of your personal data. You have the right to withdraw such consent at any time by contacting privacy@cognacity.co.uk.

8.2. Where we need to perform the contract we are about to enter into or have entered into with you or your sponsor.

8.3. Where it is necessary for our legitimate interests (or those of a third party) e.g performing a contract with your employer/sponsor, and your interests and fundamental rights do not override those interests.

8.4. Where we need to comply with a legal or regulatory obligation.

Purposes for which we will use your personal data

We have set out below, in a table format, a description of all the ways we plan to use your personal data, and which of the legal bases we rely on to do so. We have also identified what our legitimate interests are where appropriate.

Health Data requires an additional special condition to be satisfied if we are to process it lawfully. We have set out in the table below the special condition that we will satisfy in relation to the use

of your Health Data.

Note that we may process your personal data for more than one lawful ground depending on the specific purpose for which we are using your data. Please contact us via the means set out in paragraph 1.2.2 above if you need details about the specific legal ground we are relying on to process your personal data where more than one ground has been set out in the table below.

Purpose / Activity	**Type of data**	**Lawful bases for processing (including basis of legitimate interest)(Article 6)**	**Special condition for processing of Health Data (Article 9)**
To register you as a patient.	Identity Data Contact Data Financial Data Health Data	Performance of a contract with you Necessary for our legitimate interests (performing a contract with your employer).	Provision of health or social care treatment (UK GDPR, Art. 9(2)(h))
Processing of data received from GPs or other third parties.	Identity Data Contact Data Health Data	Necessary for our legitimate interests (performing a contract with you or your employer).	Provision of health or social care treatment (UK GDPR, Art. 9(2)(h)
To provide you with clinical services in accordance with the terms of any contract we have entered into with you (or your employer/sponsor).	Identity Data Contact Data Health Data	Performance of a contract with you Necessary for our legitimate interests (performing our contract with your employer/sponsor).	Provision of health or social care treatment (UK GDPR, Art. 9(2)(h))
To provide you with coaching services in accordance with the terms of any contract we have entered into with you (or your employer/sponsor).	Identity Data Contact Data Health Data	Performance of a contract with you Necessary for our legitimate interests (performing our contract with your employer/sponsor).	Provision of health or social care treatment (UK GDPR, Art. 9(2)(h))
To provide you with webinar/workshop .services in accordance with the	Identity Data Contact Data	Performance of a contract with you Necessary for our	N/A

terms of any contract we have entered into with you (or your employer/sponsor).		legitimate interests (performing our contract with your employer/sponsor).	
To provide you with Leadership assessment services in accordance with the terms of any contract we have entered into with your sponsor.	Identity Data Contact Data Profile Data	Performance of a contract with your sponsor Necessary for our legitimate interests (performing our contract with your sponsor).	N/A
To conduct an independent occupational health assessment referred by your employer, including collecting relevant information from you and preparing an assessment report.	Identity Data, Contact Data, Health Data	Necessary for our legitimate interests (performing our contract with your employer to provide the assessment)	Explicit consent (UK GDPR, Art. 9(2)(a))
To disclose the conclusions of an occupational health assessment report to your employer's named contact.	Identity Data, Health Data	Necessary for our legitimate interests (performing our contract with your employer)	Explicit consent (UK GDPR, Art. 9(2)(a))
To invoice you or a third party for our services including managing payments, fees and charges and recovering money owed to us.	Identity Data Contact Data Financial data	Performance of a contract with you Necessary for our legitimate interests (performing our contract with your employer/sponsor).	N/A
To refer externally to a third party medical professional /service provider outside of Cognacity.	Identity Data Contact Data Health Data	Performance of a contract with you Necessary for our legitimate interests (performing a	Provision of health or social care treatment (UK GDPR, Art. 9(2)(h)

		contract with your employer/sponsor).	
To provide written follow-up correspondence and referral letters to maintain continuity of care. Some administrative services are outsourced.	Identity Data Contact Data Health Data	Necessary for our legitimate interests (providing an effective service in maintaining communication with all third party clinicians and next of kin).	Provision of health or social care treatment (UK GDPR, Art. 9(2)(h)
To provide a 24/7 confidential helpline service to provide assistance in the time of crisis.	Identity Data Contact Data Health data	Performance of a contract with you (this is an implied contract as you provide the information voluntarily in order to receive this service) Necessary for our legitimate interests (performing a contract with your employer/sponsor).	Provision of health or social care treatment (UK GDPR, Art. 9(2)(h)
To manage our relationship with you including asking you to leave a review of our services or take a survey.	Identity Data Contact Data	Necessary for our legitimate interests (to keep our records updated, to ascertain how our clients use our services and to develop our services and grow our business).	N/A
To maintain clinical standards and best practice by auditing patient records periodically.	Identity Data Contact Data Health data	Necessary for our legitimate interests (to ensure all clinicians follow best practice to ensure the safety of our patients).	Provision of health or social care treatment (UK GDPR, Art. 9(2)(h)
To supplement our workshop delivery/coaching services by the use of on-line psychometric questionnaires.	Profile Data Identity Data	Performance of a contract with you or your employer/sponsor Necessary for our	Explicit Consent (UK GDPR Art 9(2)(a)

		legitimate interests (performing our contract with your employer/sponsor).	
Fulfilling our regulatory obligations (and co-operating with our regulators).	Profile Data Identity Data Health Data Contact Data	Necessary for compliance with a legal obligation to which we are subject.	Necessary for reasons of substantial public interest (UK GDPR, Art. 9(2)(g)) – (6) statutory and government purpose
Complying with a legal obligation (such as a court order requiring us to release information).	Profile Data Identity Data Health Data Contact Data	Necessary for compliance with a legal obligation to which we are subject.	Necessary for the establishment, exercise or defence of legal claim (UK GDPR, Art. 9(2)(f))
Complying with a legal obligation (such as bringing or defending a legal claim).	Profile Data Identity Data Health Data Contact Data	Necessary for compliance with a legal obligation to which we are subject.	Necessary for the establishment, exercise or defence of legal claim (UK GDPR, Art. 9(2)(f))
Anonymising personal data for the purposes of internal auditing and collating clinical data/benchmarks.	Identity Data Contact Data Health Data	Necessary for our legitimate interests (using data to benchmark our performance).	Archiving, research and statistics (UK GDPR, Art. 9(2)(j)
Keep staff, patients and premises safe and secure via use of surveillance cameras in communal areas.	Identity data	Necessary for our legitimate interests (using equipment to ensure safety of all personnel and premises).	N/A
Where there is an immediate risk of harm to an individual.	Identity data Contact Data Health Data	Necessary in order to protect the vital interests of the data subject or another natural person.	Vital Interests – Necessary to protect the vital interest of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent. UK GDPR Art. 9(2)(c)

Marketing

We strive to provide you with choices regarding certain personal data uses, particularly around marketing and advertising.

We may use your Identity Data to form a view on products or services that we think you may want or need or may be of interest to you. This is how we decide which products, services and offers may be relevant for you (we call this marketing).

You will receive marketing communications from us if you have requested information from us or engaged us to provide you with services (where you have opted in to receiving marketing communications from us).

Third-Party Marketing

We do not share your personal data with any other company for marketing purposes.

Opting-out

Should you wish to withdraw your consent to marketing, you can ask us to stop sending you marketing messages at any time by contacting us via the means set out in paragraph 1.2.2 above.

Procedure for a Data Breach

The GDPR introduces a duty to report certain types of personal data breach to the relevant supervisory authority (ICO). This will be undertaken within 72 hours of Cognacity being made aware of the breach.

If the breach is likely to adversely affect an individuals' rights and freedoms, Cognacity must also inform those individuals without undue delay. Where the services are paid for by an individual's employer, that employer will also be notified within the same time frame.

Cognacity will provide the following information to individuals when informing them about a breach:

- The nature of the personal data breach;
- The name and contact details of our data protection officer;
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach; and
- Measures taken to mitigate any possible adverse effects.

Change of Purpose

We will only use your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If you wish to get an explanation as to how the processing for the new purpose is compatible with the original purpose, please contact us via the means set out in paragraph 1.2.2 above.

If we need to use your personal data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal data without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

9. DISCLOSURES OF YOUR PERSONAL DATA

We may have to share your personal data with third parties set out below for the purposes set out in the table in paragraph 4.2.3 above. Internal Third Parties are set out in Clause 10: Glossary below.

External Third Parties are set out in Clause 10 below.

Third parties may also include companies/individuals to whom we may choose to sell, transfer or merge parts of our business or our assets. Alternatively, we may seek to acquire other businesses or merge with them. If a change happens to our business, then the new owners may use your personal data in the same way as set out in this Privacy Notice.

We require all third parties to respect the security of your personal data and to treat it in accordance with the law. We do not allow our third-party service providers to use your personal data for their own purposes and only permit them to process your personal data for specified purposes and in accordance with our instructions.

10. INTERNATIONAL TRANSFERS

When we share your personal data with Internal Third Parties or External Third Parties it may involve transferring your data outside the European Economic Area ("EEA"), to countries such as the United States of America and South Africa.

Whenever we transfer your personal data outside the United Kingdom, we ensure the same degree of protection is afforded to it, by ensuring at least one of the following safeguards is implemented:

Your personal data will be transferred to a country covered by UK adequacy regulations made by the Secretary of State under the Data Protection Act 2018 and the UK GDPR, confirming that the country provides an adequate level of protection for personal data. For any transfers to the United States of America, this is given effect through the UK Extension to the EU-U.S. Data Privacy Framework.

Where the destination country is not covered by UK adequacy regulations, which includes transfers to South Africa, we instead put in place the UK International Data Transfer Agreement (IDTA), or the EU Standard Contractual Clauses together with the UK's International Data Transfer Addendum, to ensure your personal data receives the same protection it has in the United Kingdom.

EU/EEA and Swiss Representative – Cognacity Ltd only: Cognacity Ltd processes the personal data of individuals in both the European Union and European Economic Area, in either the role of 'data controller' or 'data processor'. As such, we have appointed Data Protection Representative Ltd (trading as 'DataRep') as our Data Protection Representative for the purposes of GDPR in the EU/EEA and the Federal Act on Data Protection AS 2022 491 ('FADP') in Switzerland.

If we have processed, or are processing, your personal data, you may be entitled to exercise your rights under GDPR/FADP in respect of that personal data. For more details on the rights you have in respect of your personal data please refer to the national Data Protection Authority in your country, the European Commission in the EU (https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en) or the Federal Data Protection and Information Commission in Switzerland (https://www.edoeb.admin.ch/edoeb/en/home.html).

If you want to contact us in relation to how we are processing your data in the EU/EEA and/or Switzerland, or otherwise wish to exercise your rights in respect of your personal data, please contact DataRep direct by:

- Sending an e-mail to DataRep at datarequest@datarep.com quoting 'Cognacity Ltd' in the subject line
- Contacting DataRep on their online webform at www.datarep.com/data-request; or
- Mailing your enquiry to DataRep at the most convenient of the addresses found in the Appendix to this policy. Please note it is **ESSENTIAL** that you address your letters to 'DataRep' and not Cognacity Ltd, and clearly reference Cognacity Ltd within your correspondence.

On receiving your correspondence from DataRep, we are likely to request evidence of your identity to ensure your personal data, and any information connected with it, is not provided to anyone other than you.

11. DATA SECURITY

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. We use two-factor authentication log- ons to all Microsoft/Windows accounts and all data is encrypted at rest and in transit. Where we use third-party software, we ensure that the third-party has sufficient security measures in place. In addition, we limit access to your personal data to those employees, associates, agents, contractors and other third parties on a strict need to know basis. They will only process your personal data on our instructions and they are subject to a duty of confidentiality. All employees and associates undergo regular mandatory training in data security.

We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

12. DATA RETENTION

We will only retain your personal data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting or reporting requirements.

To determine the appropriate retention period for your personal data, we consider the amount,

nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means.

Details of retention periods for different aspects of your personal data can be obtained by contacting us via privacy@cognacity.co.uk.

In some circumstances you can ask us to delete your data: see 'Your Legal Rights' in paragraph 13 below for further information.

In some circumstances we may pseudonymise or anonymise your personal data (so that it can no longer be associated with you) for research or statistical purposes in which case we may use this information indefinitely without further notice to you.

13. YOUR LEGAL RIGHTS

Under certain circumstances, if you are an individual, you have rights under data protection laws in relation to your personal data as set out below:

13.1. Request access to your personal data (commonly known as a "data subject access request"). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.

13.2. Request correction of the personal data that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us. This does not include amendments to clinical records.

13.3. Request erasure of your personal data. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your personal data to comply with local law. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request.

13.4. Object to processing of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. You also have the right to object where we are processing your personal data for direct marketing purposes. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms.

13.5. Request restriction of processing of your personal data. This enables you to ask us to suspend the processing of your personal data in the following scenarios: (a) if you want us to establish the data's accuracy; (b) where our use of the data is unlawful but you do not want us to erase it; (c) where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims; or (d) you have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.

13.6. Request the transfer of your personal data to you or to a third party. We will provide to you, or a third party you have chosen, your personal data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you.

13.7. Withdraw consent at any time where we are relying on consent to process your personal data. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain services to you. We will advise you if this is the case at the time you withdraw your consent.

If you wish to exercise any of the rights set out above, please contact us via the means set out in paragraph 3 above.

13.8 No fee usually required: You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we may refuse to comply with your request in these circumstances.

13.9 What we may need from you: We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

13.10 Time-limit to respond: We try to respond to all legitimate requests within one month. Occasionally it may take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

14. GLOSSARY

'Comply with a legal obligation' means processing your personal data where it is necessary for compliance with a legal or regulatory obligation that we are subject to.

'*Internal Third Parties'* means our employees, associates, agents or officers engaged in the provision of our services to you.

'*External Third Parties'* means:

- Service providers acting as data processors who provide us with payment processing, IT, data protection services and system administration services.
- Professional advisers including bankers, solicitors, auditors and insurers who provide us with banking, legal, insurance and accounting services.
- HM Revenue & Customs and other authorities or regulated bodies who require reporting of processing activities in certain circumstances.
- Medical professionals and other clinical professionals in circumstances where we refer you for treatment.
- Your employer or their nominated contact, limited to the conclusions of an occupational health assessment report where you have consented to that disclosure.
- Providers who deliver administrative services/functions to assist us in running our

business and providing our services, to include secretarial services, on-line training services, HR resources and a confidential helpline service.
- Any individual deemed at risk of harm together with the police and other emergency services.

'Legitimate interest' means the interest of our business in conducting and managing our business to enable us to give you the best service and the best and most secure experience. We make sure we consider and balance any potential impact on you (both positive and negative) and your rights before we process your personal data for our legitimate interests. We do not use your personal data for activities where our interests are overridden by the impact on you (unless we have your consent or are otherwise required or permitted to by law).

'Performance of a contract' means processing your data where it is necessary for the delivery of a legal agreement to which you are either a party or a subject.

15. MONITORING AND REVIEW

Cognacity will monitor the effectiveness and review the implementation of this policy regularly, considering its suitability, adequacy and effectiveness. Our Privacy Policy reflects our commitment to protecting your personal information, ensuring transparency in how we collect and use data and upholding the highest standards of confidentiality and data security.

Any improvements identified will be made as soon as possible. Internal control systems and procedures will be subject to regular audits to provide assurance that they are effective.

Appendix

List of locations to use when mailing enquiries to DataRep when exercising your rights in respect of your personal data being processed by Cognacity Ltd in the EU/EEA or Switzerland.

Please ensure request is addressed to 'DataRep' and not Cognacity Limited

Country	Address
Austria	DataRep, City Tower, Bruckenkopfgasse 1/6. Stock, Graz, 8020, Austria
Belgium	DataRep, Rue des Colonies 11, Brussels, 1000
Bulgaria	DataRep, 25 Vitosha blvd. Fl. 2, office 4, 1000, Sofia, Bulgaria
Croatia	DataRep, Ground & 9th Floor, Hoto Tower, Savska cesta 32, Zagreb, 10000, Croatia
Cyprus	DataRep, Victory House, 205 Archbishop Makarios Avenue, Limassol, 3030, Cyprus

Czech Republic	DataRep, Platan Office, 28. Rijna 205/45, Floor 3&4, Ostrava, 70200, Czech Republic
Denmark	DataRep, Lautruph0j 1-3, Ballerup, 2750, Denmark
Estonia	DataRep, 2nd Floor, Tornimae 5, Tallinn, 10145, Estonia
Finland	DataRep, Luna House, 5.krs, Mannerheimintie 12 B, Helsinki, 00100, Finland
France	DataRep, 72 rue de Lessard, Rauen, 76100, France
Germany	DataRep, 3rd and 4th floor, Altmarkt 10 B/D, Dresden, 01067, Germany
Greece	DataRep, lppodamias Sq. 8, 4th floor, Piraeus, Attica, Greece
Hungary	DataRep, 1054 Honved street, 8 1/2, Budapest, Hungary
Iceland	DataRep, Laugavegur 13, 101 Reykjavik, Iceland
Ireland	DataRep, 77 Camden Street Lower, Dublin, D02 XE80, Ireland
Italy	DataRep, Viale Giorgio Ribotta 11, Piano 1, Rome, Lazio, 00144, Italy
Latvia	DataRep, 4th & 5th floors, 14 Terbatas Street, Riga, LV-1011, Latvia
Liechtenstein	DataRep, City Tower, Bruckenkopfgasse 1/6. Stock, Graz, 8020, Austria
Lithuania	DataRep, 44A Gedimino Avenue, 01110 Vilnius, Lithuania
Luxembourg	DataRep, BPM 335368, Banzelt 4 A, 6921, Roodt-sur-Syre, Luxembourg
Malta	DataRep, Tower Business Centre, 2nd floor, Tower Street, Swatar, BKR4013, Malta
Netherlands	DataRep, De Nieuwe Erven 3 Unit - 15162, 5431 NV Cuijk, Netherlands
Norway	DataRep, C.J. Hambros Plass 2c, Oslo, 0164, Norway
Poland	DataRep, Budynek Fronton ul Kamienna 21, Krakow, 31-403, Poland
Portugal	DataRep, Torre de Monsanto, Rua Afonso Pra<;a 30, 7th floor, Alges, Lisbon, 1495-061, Portugal
Romania	DataRep, 15 Piata Charles de Gaulle, nr. 1-T, Bucure i, Sectorul 1, 011857, Romania
Slovakia	DataRep, Apollo Business Centre II, Block E / 9th floor, 4D Prievozska, Bratislava, 821 09, Slovakia

Slovenia	DataRep, Trg. Republike 3, Floor 3, Ljubljana, 1000, Slovenia
Spain	DataRep, Calle de Manzanares 4, Madrid, 28005, Spain
Sweden	DataRep, S:t Johannesgatan 2, 4th floor, Malmo, SE - 211 46, Sweden
Switzerland	DataRep, Leutschenbachstrasse 95, ZURICH, 8050, Switzerland

POLICY SIGN OFF	
Policy name	DPS-05
Version	V4
Equality Impact assessment	No impact
Privacy impact assessment	Not relevant
Approved by	Governance and quality assurance committee
Effective from	Sept 2025
Review date	Sept 2028
Owner	Operations Manager Performance
Compliance measure	Annual spot audit

REVISION HISTORY

Version	Date	Revision Summary	Author
V1	Sept 2025	New policy	DPA/ Operations Manager Performance
V2	11 November 2025	Addition of DataRep as our EU/EEA/Swiss Data Representative	Operations Manager Performance
V3	16 December 2025	Addition of Appendix	Operations Manager Performance
V4	7 September 2026	Appendix updated with new addresses as provided by Data Rep OH Assessments now included insertion of a new clause 3.4, OH	

		assessments added as 2 new entries in table of processing, employers added as a new 'External Third Party' in the Glossary Clause 3.3 amended to include where individual being assessed is subject International Transfer clause re-worded for clarity Some reformatting of clause 13	