



OCORIAN RECRUITMENT
PRIVACY NOTICE

OCORIAN RECRUITMENT PRIVACY NOTICE

1. Introduction

This notice ("notice") sets out how we collect, manage and protect your personal data in connection with staff recruitment.

A full list of all the members of the Ocorian Group can be found at www.ocorian.com/privacy-statement-list-of-ocorian-entities.

If you have any queries regarding anything in this Notice, please contact our Group Data Protection Officer, whose contact details can be found at the end of this Notice.

2. What is Personal Information?

Your "**Personal Information**" means any information that can be used (whether alone or with other information) to identify you, the "**data subject**".

A fuller definition of "**Personal Information**" is given in Appendix 1 and lists of the kinds of Personal Information that we may process in connection with our recruitment process.

3. Where do we collect your personal information from?

- You
- Your employer/former employer/education provider
- Recruitment agencies
- LinkedIn and other job sites
- Sanctions lists and publicly accessible registers or sources of information

4. Uses and grounds on which Personal Information is processed

- Administering your application for a job with us and considering your suitability for the relevant role
- Making reasonable adjustments and equality monitoring.
- Where permitted by law, we will also conduct checks in order to verify your identity and the information in your application and obtain further information about your suitability for a role within a regulated financial services business. This may include obtaining information from your referees, regulators, and checking sanctions list and other publicly available sources of information
- Your personal information may be used as part of our talent community so that we can update you on roles and recruitment activity that may be of interest. In some cases, in order to identify suitable candidates, we may obtain your

personal information from publicly available sources such as online jobs boards of which you are a member.

We process your Personal Information using one or more of the following legal bases:

- **legitimate interests.**
 - As a regulated financial services firm, we have a legitimate interest in knowing the identity and background of the individuals we employ to ensure we have the appropriate staff to comply with our various legal and regulatory obligations and ethical duties, and in monitoring our recruitment practices in the interests of making them fair and inclusive. This includes conducting sanctions checks and checking publicly available sources of information.
 - In the context of retaining the data of unsuccessful applicants for future job opportunities, we have a legitimate interest in maintaining an appropriate pool of talent who have shown an interest in working for us and who are potentially suitable candidates for employment. This is particularly important in niche areas with a skills shortage and will potentially benefit both initially unsuccessful applicants and us.
- **Required by Law and necessary for reasons of substantial public interest**
 - Conducting background checks, verification and vetting which are necessary for the conduct of a regulated financial services business and complying with Anti-Money Laundering and Anti-Fraud legislation.
- **Your Consent**
 - Information provided for the purposes of making reasonable adjustments.

4. Storage, transfer and use of Personal Information

Your Personal Information will be stored by us as follows:

(a) if you are applying for a role in the Ocorian Group in Jersey, Ireland, the Netherlands or the United Kingdom, Personal Information collected by us is hosted in Jersey.

(b) if you are applying for a role in the Ocorian Group in Luxembourg, Personal Information collected by us is hosted on servers in a data centre provided by a third party IT service provider regulated by the Luxembourg regulator, the CSSF and if you are an employee of a member of the Ocorian Group in Luxembourg City, Personal Information collected by us is hosted on its servers at its physically-secured premises in Luxembourg City.

(c) if you are applying for a role in Singapore Trust Company or Ocorian (Mauritius) Limited, some of your Personal Information is, in addition to being held by either entity, held by Ocorian Group HR in Jersey.

(d) In addition, regardless of the jurisdiction in which you work, we use Smart Recruiters for applicant tracking management purposes and may process your Personal Information in other cloud-based and/or on-premises, third party HR systems.

(e) Third party suppliers of data centre hosting and business continuity services and of HR systems have been approved for use by Ocorian and are each subject to contractually-binding terms covering the protection of personal information, in accordance with Ocorian's Data Protection Policy.

5. Security

All members of the Ocorian Group will take appropriate measures to protect Personal Information that are consistent with EU privacy and data security laws and regulations, including requiring service providers to use appropriate measures, to protect the confidentiality and security of Personal Information.

All Ocorian companies are required to comply with all Ocorian group data protection policies. These policies impose the GDPR as a global minimum standard which ensures that personal data has the same level of protection across all Ocorian offices.

Ocorian holds the ISO27001:2022 certification for providing internal business support that includes Information Technology and Information Security services, IT Management, Legal, HR, Business Operations and Company Secretarial to the Ocorian groups

6. Retention

We will retain Personal Information for the period necessary to fulfil the purposes outlined in this Notice, typically 6 months unless a longer retention period is required or permitted by law. Retention periods are kept under review.

We may retain your data for longer if we believe we may have a future role that you may be suitable for you.

Where we rely on your consent in respect of the Personal Information you disclose during the recruitment and selection process, we will cease processing that Personal Information by deleting it if you withdraw that consent at any time.

Personal Information will be securely disposed of at the point it is no longer required.

7. Your rights

You have a number of rights in relation to your Personal Information. Under certain circumstances, you have the right to:

- a) Access to your Personal Information by making a "subject access request".
- b) Have your Personal Information corrected if it is wrong or, in certain circumstances, to have it deleted.
- c) Have the processing of your Personal Information restricted (while we verify or investigate your concerns with this information for example).
- d) Object to the further processing in certain circumstances of your Personal Information.
- e) Request we move your Personal Information elsewhere (data portability).
- f) Withdraw any consent that you have given us if we are processing your Personal Information only because you have given that consent; and
- g) Object to (1) processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling), (2) direct marketing (including profiling), and (3) processing for purposes of scientific/historical research and statistics; and
- h) Protection in respect of automated decision making and profiling.
- i) Lodge a data protection related complaint with us

8. AI Use

As part of our recruitment process, we may use artificial intelligence (AI) tools to assist with candidate screening and assessment. These tools support our decision-making, and no decisions are made solely by automated means without appropriate human oversight.

9. Ocorian contact details

If you wish to exercise any of your rights in relation to your Personal Information, have any complaints about the way in which we process Personal Information, or you require any further information about this Privacy Statement or its contents, please contact the Group Data Protection Officer, by email dpo@ocorian.com.

10. Complaints

If you have a complaint about the way in which your personal information has been processed, you have the right to contact the relevant data protection regulator but we would suggest that you first contact us first. All data protection complaints should be submitted by email dpo@ocorian.com/ We shall acknowledge the complaint within 30 days of receipt of the complaint and endeavor to provide a substantial response without undue delay.

11. Data protection regulator contacts

If your request or concern is not satisfactorily resolved by your Employer you may approach your local data protection authority in the jurisdiction in which your Employer is located.

The contact details for the data protection regulators in the jurisdictions in which members of the Ocorian group operate are as follow:

- **Bermuda:** Information Commissioner's Office, Valerie T. Scott Building, 60 Reid Street, Hamilton, Bermuda HM12. Tel: 441-294-9181. [Email: info@ico.bm](mailto:info@ico.bm)
- **British Virgin Islands:** There are currently no dedicated data protection laws in the BVI. If you have any questions, or wish to exercise any of your rights, in relation to any BVI-related data processing by Ocorian, please contact our Data Protection Officer in the first instance using the details provided above.
- **Cayman Islands:** The Ombudsman, 5th Floor, Anderson Square, 64 Shedden Road, George Town, Grand Cayman. Tel: +001345 946 6283. [Email: info@ombudsman.ky](mailto:info@ombudsman.ky)
- **Denmark:** Datatilsynet, Carl Jacobsens Vej 35, 2500 Valby, Tel: +45 33 19 32 00, dt@datatilsynet.dk
- **Dubai:** The Data Protection Commissioner, Dubai International Financial Centre Authority, Level 14, The Gate, P.O. Box 74777, Dubai, United Arab Emirates. Tel: +971 4 362 2623. [Email: administrator@dp.difc.ae](mailto:administrator@dp.difc.ae)
- **Finland:** Office of the Data Protection Ombudsman, Street address: Lintulahdenkuja 4, 00530 Helsinki, Postal address: PL 800, 00531 Helsinki, Finland, Switchboard: +358 29 566 6700, Registry: +358 29 566 6768, E-mail (registry): [tietosuoja\(at\)om.fi](mailto:tietosuoja(at)om.fi)
- **Germany:** The Federal Commissioner for Data Protection and Freedom of Information, https://bfdi.bund.de/EN/Home/EN/Service/Kontakt/kontakt_node.html
- **Guernsey:** Office of the Data Protection Authority, St Martin's House, Le Bordaige, St. Peter Port, Guernsey GY1 1BR. Tel: +44 (0)1481 742074. [Email: enquiries@odpa.gg](mailto:enquiries@odpa.gg)
- **Hong Kong:** The Office of the Privacy Commissioner for Personal Data, Room 1303, 13/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong. Tel: +852 2827 2827. [Email: enquiry@pcpd.org.hk](mailto:enquiry@pcpd.org.hk)

- **Ireland:** Office of the Data Protection Commissioner, Canal House, Station Road, Portarlington, Co. Laois, R32 AP23, Republic of Ireland. Tel: +353 (0761) 104 800, LoCall 1890 25 22 31. Email: info@dataprotection.ie
- **Isle of Man:** Isle of Man Information Commissioner, First Floor, Prospect House, Prospect Hill, Douglas, Isle of Man, IM1 1ET. Tel: +44 1624 693260 Email: ask@inforights.im
- **Jersey:** Office of the Information Commissioner, 2nd Floor, 5 Castle St, St Helier, Jersey JE2 3BT. Tel: +44 (0)1534 716530. Email: enquiries@jerseyoic.org
- **Luxembourg:** Commission nationale pour la protection des données, 1, avenue du Rock 'n' Roll, L-4361 Esch-sur- Alzette, Luxembourg. Tel. +352 (0) 26 10 60-1. Online: <https://cnpd.public.lu/en/support/contact.html>
- **Mauritius:** Data Protection Office, 5th Floor, SICOM Tower, Wall Street, Ebene, Republic of Mauritius. Tel: +(230)460-0251. Email: pmo-dpo@govmu.org
- **Netherlands:** Dutch Data Protection Authority (Autoriteit Persoonsgegevens), Bezuidenhoutseweg 30, 2594 AV The Hague, Netherlands or by post to Postbus 93374, 2509 AJ The Hague, Netherlands. Tel: +31 (0)70 888 85 00.
- **Norway:** Datatilsynet. P.O. Box 458 Sentrum, NO-0105 Oslo, Phone: +47 22 39 69 00, Email: postkasse@datatilsynet.no , Website: <https://www.datatilsynet.no/>
- **Singapore:** Personal Data Protection Commission, 460 Alexandra Road, #10-02 PSA Building, Singapore 119963. Tel: +65 6377 3131. Online: <https://www.pdpc.gov.sg/contact>
- **Sweden:** Swedish Authority for Privacy Protection's (IMY), Integritetsskyddsmyndigheten, Box 8114, 104 20 Stockholm, Sweden, Tel: +46 (0)8 657 61 00 E-mail: imy@imy.se
- **United Kingdom:** Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF. Tel: 0303 123 1113 (local rate). Online: <https://ico.org.uk/global/contact-us/>
- **United States of America:** Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Tel: +1 (202) 326-2222. Online: <https://www.ftc.gov/contact>

10. 9. Changes to this Policy

This policy may be updated periodically. Please ensure you check for the latest version regularly or contact the Group Data Protection Officer for further information

Appendix 1 - Personal Information

Types of Personal Information we may collect, use, transfer and disclose

1. **Personal Details:** Name, date of birth, contact details (email, phone number(s), residential address) languages(s) spoken, gender, information about your entitlement to work and photograph
2. **Documentation required under immigration/migration laws:** Citizenship, passport data, details of residency work permits or their equivalent.
3. **Compensation and Payroll:** Past level(s) of remuneration including benefit entitlements, compensation type, details of bonuses, commissions and other awards, working time and sickness records, (where provided to us).
4. **Work History:** Description of current and past positions, job titles, job levels, job functions, company name, branch/unit/department, location, employment status and type, hours and days worked, terms of employment, and termination date(s) and reason, length of service.
5. **Monitoring:** During the interview or applicant assessment process, we may collect information from our monitoring systems such as our access control systems, CCTV systems located at office entrances and within main corridors, online recordings using Teams or similar conferencing tools, and email communications.
6. **Work References:** Where you provide details of a personal work referee to us, we will request a personal work reference from your referee. Your referee may disclose to us information about you, your work history, your capabilities, skills, qualifications and character.
7. **Special Category & Criminal Records information:** We may also collect certain types of Special Category information only when permitted or required by local law, such as health/medical information, religion, nationality, race or ethnicity, and details of criminal convictions/offences.

We collect this information for specific purposes, such as:

- Health/medical information to accommodate reasonable adjustments to support the recruitment process.
- Diversity-related Personal Information (such as race or ethnicity) in order to comply with legal obligations and internal policies relating to diversity and anti-discrimination.
- Criminal records data to comply with legal requirements in respect of running a regulated business (anti-money laundering and anti-fraud measures, sanctions checking, “fit and proper person” tests and other offenses that may be relevant to the conduct of a regulated business).