



Colleague Privacy Notice

India

The OCS group of companies is committed to ensuring that your data and privacy are protected. This notice sets out how we will process and protect your personal information before, during, and after your working relationship with us.

OCS Group International Limited ("OCS", "we", "us", "our") is the **Data Fiduciary** responsible for your personal data in India and is committed to protecting it in accordance with the **Digital Personal Data Protection Act, 2023 ("DPDPA")** and the Digital Personal Data Protection Rules, 2025 ("DPDP Rules"). This Privacy Notice describes how we collect, use, disclose, store, and protect personal data (referred to in the DPDPA as belonging to a "Data Principal") in the course of our operations in India.

This notice applies to current and former colleagues and contractors. It does not form part of any contract of employment or other contract to provide services. We may update this notice at any time.

It is important that you read this notice so that you are aware of how and why we use your information, and how you can exercise your rights under the DPDPA.

Data Fiduciary Details

OCS Group International Limited

Thane One, A, 502, 5th Floor
Ghodbunder Road
Majiwada
Thane (West) – 400610
Maharashtra
India

Grievance Redressal Officer / Data Protection contact: Sara Taylor, Group Data Protection Officer

Email: dataprotection@ocs.com

What Personal Information Do We Collect About You?

We may collect, store, and use the following categories of personal information about you:

- Identity Data: nationality, name, title, date of birth, PAN, Aadhaar (masked, where legally required), photographs.
- Contact Data: address, contact details, IP address, and emergency contact information.
- Emergency Contact Data: relationship, contact information, details of dependant(s).
- Finance Data: bank account details, credit reference checks, payroll records, and tax records and tax status.

TRUE.Values.

© Copyright OCS / India Colleague Privacy Notice / July 2026

Internal only

- **Employment Data:** employment history, job title, flexible working requests, workplace, salary or hourly rate, benefits information, start and leaving date, maternity, paternity, parental leave and pay, contract terms and variations, and continuous service date.
- **Qualification Data:** education history, evidence of qualifications, professional memberships and licences including, where applicable, driving licence and any statutory security clearance or licence required for your role.
- **Recruitment Data:** copy of your passport, application form, referee names and contact details, curriculum vitae, proof of address documents, interview notes, right to work documentation, and references.
- **Performance Data:** probation reviews, learning and development needs/records, training records, performance reviews, appraisals, remuneration history, promotions, whistleblowing matters.
- **Disciplinary and Grievance Data:** grievance matters and records, investigation and hearing documentation, warnings/sanctions, meeting notes, audio recordings, related correspondence.
- **Monitoring Data:** information about your use of company information and communication systems, images (photographic, audio, and fixed/mobile CCTV), swipe card records, staff location tags, vehicle driving data, speed and location, and other information obtained through electronic means.
- **Absence Data:** first aid records, injury at work and third-party accident information, sickness records, special leave.

The DPDPA does not create a separate legal category of special category data — all personal data is protected in the same way under the Act. Some of the information we hold nonetheless deserves particular care, and we apply extra safeguards to it accordingly. This includes:

- Information about race or ethnicity, religious beliefs, disability status, gender identification, sexual orientation, and political opinions.
- Trade union membership.
- Information about your health and wellbeing, whether provided directly by you or obtained from health checks, occupational health referrals and reports, sick leave forms, health questionnaires, and fitness-for-work certificates.
- Accident-at-work records.
- Details of any desk audits/assessments, access needs or reasonable adjustments.
- Biometric data used for system access and/or time and attendance systems.
- Information about charges, criminal convictions and offences (see "How We Use Information About Criminal Convictions" below).

How Is Your Personal Information Collected?

We collect information about you from the following sources:

- Directly from you.
- From an employment agency.
- From your employer if you are a secondee.
- From referees, either external or internal.
- From background verification and security clearance providers.
- From occupational health and other health providers.
- From pension administrators and other government departments.
- From your trade union.

- From providers of colleague benefits.
- From CCTV, ANPR, body-worn cameras, and photographic images from our clients, landlords, or our own monitoring systems.
- From images and location data captured by door entry/exit systems.

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

What Do We Use Your Personal Information For, and On What Basis?

Under the DPDPA, we may only process your personal data where you have given consent (Section 6), or where the processing falls within one of the narrow, defined "certain legitimate uses" set out in Section 7 of the Act.

The table below sets out the main purposes for which we use your personal information and the DPDPA ground we rely on for each:

Purpose / Activity	Type of Data	DPDPA Ground for Processing
Recruitment, selection and appointment decisions, including determining the terms on which you join us.	• Identity Data • Contact Data • Recruitment Data • Qualification Data	Certain legitimate use — Section 7(i) DPDPA (employment purposes / safeguarding OCS from loss or liability)
Background checks, including verifying references, right to work in India, and required licences or qualifications.	• Identity Data • Contact Data • Recruitment Data • Qualification Data	Certain legitimate use — Section 7(i) DPDPA, and, where applicable, Section 7(c)–(e) DPDPA (legal/regulatory compliance)
Administering your contract of employment, including paying you, statutory deductions, payroll, benefits and pension arrangements.	• Identity Data • Contact Data • Finance Data • Employment Data	Certain legitimate use — Section 7(i) DPDPA, and, where applicable, Section 7(c)–(e) DPDPA (legal/regulatory compliance)
Reviewing, investigating and making decisions about your performance, role and continued engagement, including transfer to another employer as part of a business transfer.	• Identity Data • Employment Data • Performance Data • Qualification Data • Disciplinary and Grievance Data	Certain legitimate use — Section 7(i) DPDPA (employment purposes / safeguarding OCS from loss or liability)
Managing our working relationship with you, including communications, business updates and changes to our policies.	• Identity Data • Contact Data • Employment Data	Certain legitimate use — Section 7(i) DPDPA (employment purposes / safeguarding OCS from loss or liability)
Business management, reporting, planning and internal audit.	• Identity Data • Employment Data • Performance Data • Qualification Data	Certain legitimate use — Section 7(i) DPDPA (employment purposes / safeguarding OCS from loss or liability)
Performance management, appraisals, and decisions about promotion or salary review.	• Identity Data • Employment Data • Performance Data • Qualification Data	Certain legitimate use — Section 7(i) DPDPA (employment purposes / safeguarding OCS from loss or liability)

Purpose / Activity	Type of Data	DPDPA Ground for Processing
Arrangements for the end of our working relationship, including any termination payments.	- Identity Data - Employment Data - Contact Data - Finance Data	Certain legitimate use — Section 7(i) DPDPA (employment purposes / safeguarding OCS from loss or liability)
Disciplinary and grievance investigations, hearings and related record-keeping.	- Identity Data - Contact Data - Employment Data - Performance Data - Disciplinary and Grievance Data - Monitoring Data	Certain legitimate use — Section 7(i) DPDPA (employment purposes / safeguarding OCS from loss or liability)
Providing colleague information to a new service provider where your role transfers as part of a business or contract transition.	- Identity Data - Employment Data	Certain legitimate use — Section 7(i) DPDPA (employment purposes / safeguarding OCS from loss or liability)
Handling legal claims, regulatory investigations and disputes involving you or other colleagues, including road traffic matters involving a company vehicle.	- Identity Data - Contact Data - Employment Data - Performance Data - Qualification Data - Disciplinary and Grievance Data - Monitoring Data	Certain legitimate use — Section 7(c)–(e) DPDPA (compliance with a judgment/order, or a disclosure obligation under law)
Protecting your health, safety and wellbeing and meeting our health and safety obligations.	- Identity Data - Monitoring Data - Health Data	- Certain legitimate use — Section 7(i) DPDPA, and, where applicable, Section 7(c)–(e) DPDPA (legal/regulatory compliance) - Where health data is collected beyond what is needed for a safety or legal obligation (e.g. voluntary wellbeing programmes), we will ask for your consent — Section 6 DPDPA.
Fraud prevention.	- Finance Data - Identity Data	Certain legitimate use — Section 7(i) DPDPA, and, where applicable, Section 7(c)–(e) DPDPA (legal/regulatory compliance)
Monitoring use of company information and communication systems to protect network and information security.	- Monitoring Data - Identity Data - Performance Data	Certain legitimate use — Section 7(i) DPDPA (employment purposes / safeguarding OCS from loss or liability)
Monitoring company vehicles (GPS location, driver behaviour) using telematics and forward/rear-facing dash cams.	- Monitoring Data - Identity Data - Employment Data - Performance Data	Certain legitimate use — Section 7(i) DPDPA (employment purposes / safeguarding OCS from loss or liability)
Managing attendance and presence at office or customer sites (e.g. ANPR, access control and time-and-attendance systems).	- Monitoring Data - Identity Data	Certain legitimate use — Section 7(i) DPDPA (employment purposes / safeguarding OCS from loss or liability)

Purpose / Activity	Type of Data	DPDPA Ground for Processing
Colleague data analytics, for example to better understand retention and attrition.	- Identity Data - Employment Data - Performance Data	Certain legitimate use — Section 7(i) DPDPA (employment purposes / safeguarding OCS from loss or liability)
Staff location technology used to support fair task allocation, proof of task completion, colleague safety and accurate time and attendance.	- Monitoring Data - Identity Data - Performance Data	Certain legitimate use — Section 7(i) DPDPA (employment purposes / safeguarding OCS from loss or liability)

Where none of the above grounds is available — for example, optional wellbeing initiatives, or uses of your data that go beyond what is reasonably needed for your employment — we will ask for your specific, informed consent before processing your data for that purpose.

If You Fail to Provide Personal Information

If you fail to provide certain information when requested, we may be unable to administer aspects of your employment (such as paying you or providing a benefit), or we may be unable to comply with our legal obligations (such as those relating to your health and safety).

Change of Purpose

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another compatible reason. If we need to use your personal information for a new, unrelated purpose, we will provide you with an updated notice and, where the DPDPA requires it, seek your fresh consent before doing so. We may process your personal information without a fresh notice or consent where this is otherwise permitted under Section 7 of the DPDPA.

Do We Need Your Consent to Use Your Personal Information?

Not always. We only need to ask for your consent where the processing does not fall within one of the certain legitimate uses set out in Section 7 of the DPDPA. In practice, this means we do not usually need to ask for separate consent to:

- carry out activities that are necessary for the purposes of your employment, or to safeguard OCS from loss or liability (Section 7(i));
- comply with a judgment, decree, order, or a legal obligation to disclose information (Section 7(c)–(e)).

Where we do rely on your consent — for example, for optional wellbeing programmes or other uses outside the scope of Section 7 — that consent will be free, specific, informed, unconditional and given through clear affirmative action, and you may withdraw it at any time.

How We Use Information About Criminal Convictions

We will only use information relating to criminal charges, convictions and offences where the DPDPA permits us to do so — generally under Section 7(i), where this is necessary for employment purposes such as vetting for a specific role, or with your consent under Section 6. We will only collect this information where it is appropriate given the nature of the role, for example as part of the recruitment process, or where you notify us of it directly during your employment.

Automated Decision-Making

We do not currently make any decisions about you using solely automated means without human involvement. If this position changes, we will notify you in writing.

Data Sharing — When We May Need to Share Your Personal Information with Third Parties

We may share your personal information with third parties where this is necessary for employment purposes, to comply with the law, or with your consent. Your data may be processed outside India as part of our business process outsourcing arrangements — see "Transferring Information Outside India" below.

Who Might We Share Your Personal Information With?

We will share your personal information:

- with any supplier or client used in the recruitment process, or while vetting applicants and colleagues;
- with third-party goods and/or service providers (including contractors and designated agents) for pension administration, benefits, training, uniforms, vehicle suppliers and hire companies, IT services, ID badges and passes, access to client-controlled premises, company surveys, courts, regulators, and professional advisers;
- with life assurance and health insurance providers;
- with credit reference agencies for credit reference, fraud prevention and anti-money-laundering checks;
- with current and potential clients with whom you have or may have contact, and their professional advisers;
- with industry bodies with whom you have collective agreements, or for learning, training, development or qualification purposes;
- with a prospective seller or buyer if we sell or buy any business or assets;
- where we are under a duty to disclose or share your personal data to comply with a legal obligation, enforce a legal agreement, or protect the rights, property or safety of our clients, ourselves or others;
- with other entities in the OCS group;
- in connection with any driving or parking fine, penalty or notice where we are asked to provide driver details;
- with financial wellbeing providers.

How Do We Keep Information Shared with Third-Party Service Providers and Other OCS Group Entities Safe?

All our third-party service providers and other entities in the OCS group are required to take appropriate security measures to protect your personal information, in line with our policies and the DPDPA. We do not allow third parties to use your personal data for their own purposes; we only permit them to process it for specified purposes and in accordance with our instructions, as required for Data Processors under the DPDPA.

When We May Share Your Personal Information

We will share your personal information with a third-party business support organisation to administer your contract of employment, process payments to you, process benefits, manage work deployment, and process learning and development, disciplinary and related matters, as part of our regular reporting on company

performance, in the context of a business reorganisation or restructuring exercise, and for system maintenance, support and hosting of data.

We may share your personal information with other third parties, for example in the context of a possible sale, transfer or restructuring of the business. We may also need to share your personal information with clients, prospective clients, government agencies, regulators, or otherwise to comply with the law.

In some circumstances, a client with whom you work, have worked, or may have contact (and their professional advisers) may ask us to provide your personal information for the purposes of an audit, compliance review, or evaluation of the services we provide. Where information of a more sensitive nature is requested, and we do not already have a basis to share it under Section 7 of the DPDPA, we will ask for your consent before disclosing it.

We may be asked to provide your name, work experience and qualifications to existing or potential clients. Where we act as sub-contractors on projects and facilities management jobs, we may need to provide training certificates, employment history, CV and contact information to the client/main contractor to meet health and safety obligations.

Transferring Information Outside India

Section 16 of the DPDPA permits the transfer of personal data outside India, except to any country or territory that the Central Government specifically restricts by notification. Where your personal data is transferred outside India — for example, as part of our business process outsourcing or group IT arrangements — we will take all steps reasonably necessary to ensure it continues to be treated securely and in line with this notice, and we will not transfer your data to a country restricted by the Central Government.

How Do We Keep Your Data Safe?

We are committed to keeping your information secure and take reasonable security safeguards in line with the DPDPA and DPDP Rules to prevent unauthorised access, use or disclosure. These include:

- storing your electronic personal data on secure servers or in a secure cloud environment, using encryption or masking where appropriate;
- access controls, access logging and monitoring of our systems;
- maintaining backups and other measures to preserve continued processing in the event of a data breach;
- providing colleagues with regular data protection and information security awareness training;
- keeping paper records to a minimum, and storing those we do have in locked filing cabinets, desks, or archived storage;
- maintaining up-to-date firewalls and anti-virus software; and
- enforcing a strict policy on the use of mobile devices and out-of-office working.

Third parties will only process your personal information on our instructions and where they have agreed to keep it confidential and secure.

We have procedures in place to detect and deal with any suspected personal data breach. In the event of a breach, we will notify the Data Protection Board of India and affected colleagues without undue delay, in line with the timelines set out in the DPDP Rules.

How Long Is Your Personal Information Kept?

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including to satisfy legal, accounting or reporting requirements. Details of retention periods are available in our Retention Policy, available on our intranet or on request from the Grievance Redressal Officer / Data Protection contact. Your line manager can also supply you with a copy.

To determine an appropriate retention period, we consider the amount, nature and sensitivity of the data, the potential risk of harm from unauthorised use or disclosure, the purposes for which we process it and whether those purposes can be achieved by other means, and applicable legal requirements. Where the DPDP Rules require it, we will notify you before your personal data is erased.

In some circumstances, we may anonymise your personal information so that it can no longer identify you, in which case we may use it without further notice to you.

Once you are no longer a colleague, we will retain and securely erase your personal information in accordance with our Retention Policy.

Your Rights and How You Can Control the Information We Hold About You

The DPDPA gives you the following rights as a Data Principal:

- **Right to access information** (Section 11) — to request a summary of the personal data we hold about you and the processing activities we carry out, including the identities of any Data Processors and other Data Fiduciaries with whom your data has been shared.
- **Right to correction and erasure** (Section 12) — to ask us to correct inaccurate or incomplete personal data, or to update it, and to ask us to erase personal data that is no longer necessary for the purpose it was collected for. We may need to retain some data where the law requires it, even if you request erasure.
- **Right to grievance redressal** (Section 13) — to raise a concern with us about how we handle your personal data (see "Grievance Redressal / Data Protection Contact" below).
- **Right to nominate** (Section 14) — to nominate another individual to exercise your rights on your behalf in the event of your death or incapacity.
- **Right to withdraw consent** — where processing is based on your consent you can withdraw it at any time.

These rights do not apply in all cases, particularly where personal data must be processed and/or retained for legitimate, legal or regulatory reasons. If you want to exercise any of these rights, please contact our Grievance Redressal Officer / Data Protection contact in writing. We may need to verify your identity before we can act on your request.

We aim to resolve grievances promptly, and in any event within the period set out in our grievance redressal system, which will not exceed ninety days. If you remain unsatisfied after raising a grievance with us, you may complain to the Data Protection Board of India, whose details are published by the Ministry of Electronics and Information Technology at www.meity.gov.in.

Your Duty to Inform Us of Changes

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes (such as a change of name, address or bank details) during your working relationship with us.

Right to Withdraw Consent

Where you have given your consent to the collection, processing or transfer of your personal information for a specific purpose, you have the right to withdraw that consent at any time, as easily as you gave it. Withdrawal will not affect the lawfulness of processing carried out before you withdrew consent and will not affect any processing we carry out on a different lawful ground. Please contact our Grievance Redressal Officer / Data Protection contact at dataprotection@ocs.com.

Grievance Redressal / Data Protection Contact

If you have any questions about this notice or how we handle your personal information, or wish to raise a grievance, please contact our Grievance Redressal Officer / Data Protection contact:

- by email at: dataprotection@ocs.com

If your grievance remains unresolved, you are also entitled to complain to the Data Protection Board of India.

How We Keep This Notice Up to Date

We will review and update this notice as required, to reflect a change to our internal procedures or a change in the law. The most current version of this notice will govern our processing of your personal data.

Policy Name: Colleague Privacy Notice for India Colleagues

Policy Owner: Group Data Protection Officer

Version: 1.0

Date: 1 July 2026