COPENHAGEN OFFSHORE PARTNERS

COP

Privacy Policy

COPENHAGEN OFFSHORE PARTNERS

Contents

COPENHAGEN OFFSHORE PARTNERS

1. Purpose and Scope

In connection with your engagement with Copenhagen Offshore Partners ("COP," "our," or "us"), we will, as a 'data controller', collect and process personal data about you.

The privacy regulations across the various locations we operate, requires us to provide you with information about how we collect, process, and disclose your personal data, which categories of personal data we process and the purposes for such processing.

2. Categories of personal data we process

The types of personal data we process depends on your relationship with us. Below is a list of the categories of personal data we process, for each "Data Subject".

<table>
<tr><th colspan="2">Categories of Data Subjects and categories of personal data</th></tr>
<tr><td>Data Subjects</td><td>Personal Data We Collect</td></tr>
<tr><td>Former Employees</td><td><u>Special categories of personal data that we process</u>
☐ Racial or ethnic origin ☐ Philosophical beliefs
☐ Political Opinions ☐ Trade union membership ☐ Sex life or sexual orientation
☐ Religious Beliefs ☐ Health Data ☐ Genetic or biometric data for the purpose of identification
☒ Criminal convictions and offenses and related security measures

☒ <u>Non Sensitive categories of personal data that we process</u>

Name, address, e-mail address, mobile telephone number, national identification number (CPR or other relevant number) or other government or state issue IDs, job application, CV, your photo, education papers and exam transcripts, result of personality test, references from previous employers and other nominated references, employee ID, employment contract, additions to contracts, salary adjustments, bonus, tax information, unemployment fund sworn statements regarding sick leave, annual appraisals, copy of passports of those traveling (incl. passport number and national identification number), certificates for completed education and course attendance, photos/videos from company events, civil status, information on relatives and family (including passport numbers and national identification numbers in the case of spouses or partners), warnings and termination of employment and relevant background information, potential disputes, bank account details, Nem Account number, credit card numbers, pension provider, pension contribution, frequent flyer information, log of IP addresses, log of access to files online, on servers or computers, specifying employee ID and access time, first aid records, injury at work & third party accident information, evidence of right to work and or immigration status, other specifics (if applicable). These data are retained for a specific period according to local laws.</td></tr>
<tr><td>Current Consultants on individual contracts</td><td><u>Special categories of personal data that we process</u>
☐ Racial or ethnic origin ☐ Philosophical beliefs
☐ Political Opinions ☐ Trade union membership ☐ Sex life or sexual orientation
☐ Religious Beliefs ☐ Health Data ☐ Genetic or biometric data for the purpose of identification
☒ Criminal convictions and offenses and related security measures

☒ <u>Non-sensitive categories of personal data:</u></td></tr>
</table>

Categories of Data Subjects and categories of personal data

Data Subjects	*Personal Data We Collect*
	Name, address, e-mail address, mobile telephone number, national identification number (CPR or other relevant number), job application, CV, your photo, education papers and exam transcripts, result of personality test, references from previous employers and other nominated references, employee ID, additions to contracts, salary adjustments, bonus, tax information, unemployment fund, sworn statements regarding sick leave, copy of passports of those traveling (incl. passport number and national identification number), certificates for completed education and course attendance, civil status, information on relatives and family, potential disputes, bank account details, credit card numbers, frequent flyer information.
Job Candidates	**Special categories of personal data that we process** ☐ Racial or ethnic origin ☐ Philosophical beliefs ☐ Political Opinions ☐ Trade union membership ☐ Sex life or sexual orientation ☐ Religious Beliefs ☐ Health Data ☐ Genetic or biometric data for the purpose of identification ☒ Criminal convictions and offenses and related security measures ☒ **Non-sensitive categories of personal data:** Name, address, date of birth, legal gender, telephone number, e-mail address, education, photograph, career history, recommendations/references, residency, copies of right-to-work documentation and other information included in a CV or cover letter or as part of the application process, interview and assessment details, and pre employment screening data.
Third parties (i.e., Suppliers, Customers, Business Partners)	**Special categories of personal data that we process** ☐ Racial or ethnic origin ☐ Philosophical beliefs ☐ Political Opinions ☐ Trade union membership ☐ Sex life or sexual orientation ☐ Religious Beliefs ☐ Health Data ☐ Genetic or biometric data for the purpose of identification ☒ Criminal convictions and offenses and related security measures ☒ **Non-sensitive categories of personal data:** Professional Contact details (name, work telephone, work email address, work address).
Visitors to our website	**Special categories of personal data that we process** ☐ Racial or ethnic origin ☐ Philosophical beliefs ☐ Political Opinions ☐ Trade union membership ☐ Sex life or sexual orientation ☐ Religious Beliefs ☐ Health Data ☐ Genetic or biometric data for the purpose of identification ☐ Criminal convictions and offenses and related security measures ☒ **Non-sensitive categories of personal data:** Device information such IP address, location, browser type and language, the uniform resource locator (URL), access times, viewed & clicked pages, user searches. • Please also refer to our cookie policy
Visitors to Our Offices	**Special categories of personal data that we process** ☐ Racial or ethnic origin ☐ Philosophical beliefs ☐ Political Opinions ☐ Trade union membership ☐ Sex life or sexual orientation ☐ Religious Beliefs ☐ Health Data ☐ Genetic or biometric data for the purpose of identification ☐ Criminal convictions and offenses and related security measures

Categories of Data Subjects and categories of personal data	
Data Subjects	***Personal Data We Collect***
	☒ **Non-sensitive categories of personal data:** Professional Contact details (name, work telephone, work email address, work address), photos, videos [CCTV -if allowed by country law].
Participants to Company Events	**Special categories of personal data that we process** ☐ Racial or ethnic origin ☐ Philosophical beliefs ☐ Political Opinions ☐ Trade union membership ☐ Sex life or sexual orientation ☐ Religious Beliefs ☐ Health Data ☐ Genetic or biometric data for the purpose of identification ☐ Criminal convictions and offenses and related security measures ☒ **Non-sensitive categories of personal data:** Professional Contact details (name, work telephone, work email address, work address), photos, videos, other specifics (if required)
Whistleblowers	• Please refer to COP's Whistleblower Policy

3. Purposes of our Processing of Personal Data

We process personal data for different purposes, depending on your relationship with us. We ensure that all data processing activities are conducted transparently and in accordance with applicable data protection laws as mentioned in Appendix 1 - Applicable Privacy Regulations & Authorities per location.

Purposes for our Processing of Personal Data	
Data Subject	***Purposes for Processing***
Former Employees and Former Consultants on individual contracts	☒ Documentation of reports towards / from authorities (in the case of former employees only) ☒ Documentation of the established pension or insurance scheme and payment of such ☒ Documentation of vacation and leave as well as absence due to pregnancy ☒ Documentation of any collaborative problems, complaints and warnings ☒ Documentation of termination ☒ For the enforcement of legal requirements in the event of a dispute or a claim against you ☒ Compliance with privacy laws: legal documentation requirements, basic principles and legal grounds, investigating and reporting suspected personal data breaches, handling requests and complaints from data subjects and others, handling inspections and queries by supervisory authorities, handling disputes with data subjects and third parties
Job candidates	☒ Application collection: Gathering resumes, cover letters, and application forms submitted by candidates. ☒ Screening & Shortlisting: Reviewing applications to shortlist candidates based on qualifications and experience. ☒ Background checks: Conducting background checks, including employment history, education verification, and criminal record checks (if permitted by local laws) ☒ Interview Scheduling: Coordinating and scheduling interviews with candidates

Purposes for our Processing of Personal Data	
Data Subject	***Purposes for Processing***
	☒ Assessment and Testing: Administering skills tests, personality assessments, and other evaluations ☒ Interview Feedback: Collecting and processing feedback from interviewers ☒ Offer Management: Preparing and sending job offers, and managing negotiations ☒ On Boarding preparation: Collecting necessary documents and information for on boarding new hires
Third parties (e.g. Suppliers, Customers, Business Partners, Individual contractors)	☒ Third party registration: Collecting and storing personal details such as names, contact information, and business credentials ☒ Contract Management: Processing contracts, agreements, and related documents ☒ Payment processing: Managing bank details, processing invoices, and handling payments ☒ Invoicing processing: Preparation of invoices and proof of execution ☒ Performance monitoring: Evaluating performance and maintaining records of interactions and transactions ☒ Compliance & Audits: Ensuring compliance with legal and regulatory requirements, including conducting audits ☒ Health & Safety Compliance: Recording health data, managing workplace safety incidents, and ensuring compliance with health regulations ☒ Communication Management: Storing and managing communication records, including emails and meeting note ☒ Risk Management: Assessing and managing risks associated with suppliers, including background checks ☒ Know your Counterparty requirements: Ensuring compliance with KYC requirements ☒ Compliance with privacy laws: legal documentation requirements, basic principles and legal grounds, investigating and reporting suspected personal data breaches, handling requests and complaints from data subjects and others, handling inspections and queries by supervisory authorities, handling disputes with data subjects and third parties
Visitors to our offices	☒ Visitor Registration: Collecting personal details such as names, contact information, and purpose of visit ☒ Identification Verification: Checking identification documents like ID cards or passports ☒ Access Control: Issuing visitor badges and managing access to different areas within the premises ☒ Visit Logs: Recording entry and exit times for security and compliance purposes ☒ Health and Safety Compliance: Collecting health-related information, such as COVID-19 vaccination status or recent travel history (if required by law) ☒ Surveillance: Monitoring and recording video footage through CCTV systems (if allowed by law) ☒ Communication Records: Storing communication details, such as emails or phone calls related to the visit (only on a need to have basis)
Visitors to our website	☒ Analyse user clicks and usage of the application and website to improve user experience and maximize usage of our services. ☒ Manage our website and application to maintain and deliver the contracted functionality and services. ☒ Prevent fraud and other prohibited or illegal activities. ☒ Protect the security or integrity of the website, application, our business or services. ☒ Or otherwise, as disclosed to you at the point of collection or as required or permitted by law.
Participants to Company Events	☒ Registration & Ticketing: Collecting names, email addresses, and payment information for event registration ☒ Communication: Sending event details, updates, and reminders via email or other electronic means ☒ Attendee Management: Creating and managing attendee lists, including dietary requirements and accessibility needs ☒ Badge Printing: Printing name tags and badges with personal information. ☒ Feedback Collection: Gathering post-event feedback through surveys and questionnaires ☒ Marketing & Promotion: Using personal data for promotional activities, such as featuring speakers' headshots and bios, photos of the event, etc ☒ Health and Safety Compliance: Collecting health-related information, such as vaccination status or recent travel history (if required by law) ☒ Security and Access Control: Managing access to the event venue and monitoring through CCTV (if allowed by law).
Whistleblowers	☒ Please refer to COP's Whistleblower Policy

4. How we Collect Personal Data

Personal data is primarily collected by us directly from you. In the following cases, we collect personal data from related COP group entities or from third parties:

- For recruitment purposes we may collect personal data (CVs) via recruitment agencies, referrals and job websites (e.g. LinkedIn).
- For pre-employment checks we may collect personal data via authorized third parties (if required & permitted by law).
- During a company event we obtain photographs/videos for the photographer/videographer who has taken the photographs.

When we collect personal data directly from you for any of the purposes outlined above at section 3, you provide the personal data on a voluntary basis or in order for us to comply with the law, or to enter into or fulfill a contract with us, or a third party. Whether or not you are under an obligation to provide us with such personal data will depend on the specific circumstances.

The consequences of not providing the personal data are that we cannot fulfil the abovementioned purposes, including that we cannot fulfil our obligations to you or that we cannot fulfil our obligations to public authorities.

5. The Legal Basis for Processing of Personal Data

There are several legal bases on which we process your personal data. The legal bases on which we process your personal data are:

Legal Basis for Processing of Personal Data	
Contractual Necessity	The processing of your personal data is essential for the execution and fulfillment of a contract to which you are a party. This means that without processing your data, we would not be able to perform our contractual obligations or provide the services you have requested.
Legal Compliance	The processing of your personal data is required to comply with legal obligations that COP must adhere to. This includes any laws, regulations, or legal processes that mandate the collection, storage, and use of your data.
Legitimate Interests	The processing of your personal data is necessary for the purposes of legitimate interests pursued by COP or a third party. These interests could include improving our services, ensuring the security of our systems, or conducting business operations efficiently. We ensure that these interests do not override your fundamental rights and freedoms.

Legal Claims	The processing of your personal data is necessary to establish, exercise, or defend legal claims. This means that we may need to use your data in the context of legal proceedings, whether to protect our rights, respond to claims against us, or comply with court orders.
Consent	The processing of your personal data is based on your explicit consent. This means that you have given us clear permission to process your data for specific purposes. You have the right to withdraw your consent at any time, and we will cease processing your data for those purposes unless there is another legal basis for doing so.

6. Disclosure of Personal Data to Other Entities

We may disclose personal data to, and share personal data with, the following recipients in the ordinary course of our business.

Disclosure of Personal Data to Other Entities
☒ Public Authorities*: Government bodies and regulatory agencies.*
☒ Pension Funds*: Organizations managing retirement funds.*
☒ Insurance Companies*: Providers of insurance services.*
☒ Marketing Companies: *Firms specializing in marketing and advertising.*
☒ Travel Agencies*: Businesses arranging travel services.*
☒ Accountants and Legal Advisors*: Professionals providing accounting and legal services.*
☒ Other Relevant Advisors and Cooperating Partners: *Various consultants and business partners.*
☒ Law Enforcement*: In cases of suspected criminal offenses, information may be disclosed to the police or other relevant parties.*
☒ COP Affiliated Companies*: Other companies within the COP group.*
☒ Third-Party Entities: *Organizations required to fulfill their Know Your Customer (KYC) obligations.*
☒ Potential Investors*: Individuals or entities interested in investing in our business.*

The personal data is disclosed in connection with fulfilling the purposes described in section 3. The legal basis on which we disclose or share your personal data are according to the legal basis as described in section 5.

7. Withdrawal of Consent

When the processing or transfer of personal data is based on your consent, which will be collected separately, you have the right to withdraw your consent to the processing, disclosure or transfer of your personal data. If you withdraw the consent, this will not affect the lawfulness of the processing and disclosure prior to the withdrawal, but we will no longer use your consent as a legal basis for any processing of your personal data. Please contact us using the contact details in section 12 if you wish to exercise this right related to any consents, which we may have obtained from you.

8. Transfer of Personal Data to 'data processors'.

We use a number of 'data processors' who provide systems and services to us. As part of the provision of systems and services, these 'data processors' may process your personal data. These 'data processors' include, but are not limited to, the following entity categories:

- IT service providers who offer IT systems and tools and store personal data on our behalf
- Payroll administration providers
- Providers of online communication and file storage platforms
- Providers of personality and cognitive ability tests

9. International Transfers of Personal Data to Recipients (both 'data controllers' and 'data processors') in countries outside the EU/EEA

We may transfer your personal data to recipients, including both 'data controllers' and 'data processors', located in countries outside the European Union (EU) and the European Economic Area (EEA). These transfers are necessary for the performance of our services and to fulfil our contractual obligations.

Recipients of Personal Data:

- Data Controllers: Entities that determine the purposes and means of processing your personal data.
- Data Processors: Entities that process personal data on behalf of data controllers.

Countries Outside the EU/EEA:

We ensure that any transfer of personal data to countries outside the EU/EEA is conducted in compliance with applicable data protection laws. This includes implementing appropriate safeguards to protect your personal data.

Safeguards for International Transfers:

- **Adequacy Decisions:** Transfers to countries that have been recognized by the European Commission as providing an adequate level of data protection.
- **Standard Contractual Clauses (SCCs)**: Using SCCs approved by the European Commission to ensure that personal data transferred outside the EU/EEA is protected.
- **Binding Corporate Rules (BCRs):** Implementing BCRs for intra-group transfers of personal data within our corporate group.

- **Other Legal Mechanisms:** Utilizing other legal mechanisms as required by applicable data protection laws.

10. Retention Period

We store personal data for as long as necessary to fulfill the purposes outlined above. The retention periods for personal data are defined by local regulations and the need to have a legitimate basis for retaining the data. In specific cases, personal data may be retained for a longer duration if there is an ongoing dispute.

If personal data are no longer relevant, we delete them once their purposes for processing have been achieved.

11. How We Secure Personal Information

We protect the security of all of the personal information we collect and use. We use a variety of physical, administrative and technical safeguards designed to help protect it from unauthorized access, use and disclosure. We have implemented best-practice standards and controls in compliance with internationally recognized security frameworks. We use encryption technologies to protect data at rest and in transit.

12. Your Rights

As a data subject, you have several important rights regarding your personal data.

You have the right to access your data and obtain information about how it is being processed. You can request corrections if your data is inaccurate or incomplete. Additionally, you have the right to request the deletion of your data under certain conditions, such as when it is no longer needed for the purposes for which it was collected. You can also object to the processing of your data or request restrictions on how it is used. If you have provided consent for data processing, you have the right to withdraw that consent at any time. To exercise any of these rights, you may contact us at compliance@cop.dk or via post (Adress: Gdanskgade 18, 2150 Nordhavn, Copenhagen, Denmark). We will respond to your request as required by the relevant privacy laws. You have the right to lodge a complaint to the Danish Data Protection Agency or / and or to the relevant to your country authority if you believe your data protection rights have been violated.

You may also review your rights based on your location by using the table in the Appendix 1 and click to the link of your country authority.

Handling your requests

- Submission of Requests: Requests can be made in writing, using our Information Request Form or any other preferred method. You may also send requests to COP via our Webpage / Contact us [https://www.cop.dk/contact/] , or via post Gdanskgade 18, 2150 Nordhavn, Copenhagen, Denmark.
- Verification of Identity: We verify the identity of the requester to ensure data is only provided to the correct individual. Acceptable IDs include passports, driver's licenses, and national identity cards.
- Acknowledgment of Receipt: We acknowledge receipt of DSRs within 5 business days.
- Assessment and Response: We assess and respond to valid requests within 30 days. For complex requests, we may extend this by an additional 60 days, informing the requester of the extension and reasons.
- Implementation: Approved requests will be fulfilled by providing access, correcting inaccuracies, or deleting data. If denied, we will explain the reasons and how to lodge a complaint with the supervisory authority.
- Record Keeping: We maintain records of all DSRs, including the nature of the request, identity verification, and actions taken.

13. Data Breach Notification

In the event of a data breach, we are committed to taking immediate and appropriate action to mitigate any potential harm. We will promptly notify affected individuals if their personal data has been compromised, providing clear information about the nature of the breach and the steps they can take to protect themselves. We will also report the breach to relevant regulatory authorities as required by law if required. Our priority is to ensure the security of your personal data and to prevent future breaches through continuous improvement of our security measures. If external parties experience a potential data breach please reach out to COP Compliance at compliance@cop.dk. Alternatively, you can submit your report anonymously or confidentially through our Speak Up! Platform, accessible on our website at www.cop.dk.

14. Data Controller

The data controller for your personal data is COP Group Companies, which includes our headquarters, branches, and subsidiaries. The specific COP entity acting as the data controller depends on the nature of the processing activity. For more information about which entity is the data controller for your data, please contact us at compliance@cop.dk.

15. Policy Review, Monitoring and Approval

COP reserves the right to amend and revise the content of this policy when necessary (e.g., legislative changes, COP business changes). At a minimum, COP will initiate a review of this Policy every two (2) years. This policy is approved by the Chief Financial Officer of COP A/S.

16. Contact & Complaints

Should you have any questions, feedback, or complaints about this Privacy Policy, please send an email to compliance@cop.dk or via post (Gdanskgade 18, 2150 Nordhavn, Copenhagen, Denmark). You also have the right to complain to the Danish Data Protection Agency or / and to relevant local regulatory authorities in relation to your rights and about COP's processing of your personal data.

17. Policy Versions

The following table illustrates version logs and respective changes of this policy.

Version No	Effective from	Changes	Approved by
1	December 2024	Policy updates/additions for data subjects & local country law requirements	Chief Financial Officer COP A/S

COPENHAGEN OFFSHORE PARTNERS

APPENDIX 1 : Applicable Privacy Regulations & Authorities per location.

Country	Regulation, Authority and Data Breach Notification Time
Australia	Regulation: Privacy Act 1988. Authority: Office of the Australian Information Commissioner (OAIC) Data breach notification time: As soon as practicable, ideally within 72 hours
Brazil	Regulation: Lei Geral de Proteção de Dados (LGPD) Authority: The Autoridade Nacional de Proteção de Dados (ANPD), or National Data Protection Authority Data breach notification time: Within 2 working days
Denmark	Regulation: General Data Protection Regulation (GDPR) and the Danish Data Protection Act Authority: Danish Data Protection Agency [Datatilsynet] Data breach notification time: Within 72 hours
France	Regulation: General Data Protection Regulation (GDPR) and the French Data Protection Act (Loi Informatique et Libertés) Authority: Commission Nationale de l'Informatique et des Libertés (CNIL) Data breach notification time: Within 72 hours
Germany	Regulation: General Data Protection Regulation (GDPR) and the Federal Data Protection Act (BDSG) Authority:Federal Commissioner for Data Protection and Freedom of Information (BfDI) Data breach notification time: Within 72 hours
Greece	Regulation: General Data Protection Regulation (GDPR) and several national laws, including Law 4624/2019 and Law 3471/2006 Authority: Hellenic Data Protection Authority (HDPA) Data breach notification time: Within 72 hours
India	Regulation: Digital Personal Data Protection (DPDP) Act Authority: Data Protection Board of India (CERT-in) Data breach notification time: Within 6 hours
Italy	Regulation: General Data Protection Regulation (GDPR) and the Italian Personal Data Protection Code (Codice in Materia di Protezione dei Dati Personali) Authority: Garante per la Protezione dei Dati Personali (Garante Privacy) Data breach notification time: Within 72 hours
Japan	Regulation: Act on the Protection of Personal Information (APPI) Authority: Personal Information Protection Commission (PPC) Data breach notification time: Immediately, usually within 3 to 5 days, detailed report within 30 days
Netherlands	Regulation: General Data Protection Regulation (GDPR) and the Dutch GDPR Implementation Act (Uitvoeringswet Algemene Verordening Gegevensbescherming, UAVG) Authority: Autoriteit Persoonsgegevens (AP), also known as the Dutch Data Protection Authority. Data breach notification time: Within 72 hours
New Zealand	Regulation: Privacy Act 2020 Authority: Office of the privacy Commission Data breach notification time: As soon as practicable, ideally within 72 hours
Philippines	Regulation: Data Privacy Act of 2012 Authority: National Privacy Commission (NPC) Data breach notification time: Within 72 hours
Portugal	Regulation: General Data Protection Regulation (GDPR) and Law no 58/2019 Authority: Comissão Nacional de Proteção de Dados (CNPD) Data breach notification time: Without undue delay, where feasible, within 72 hours
South Korea	Regulation: Personal Information Protection Act (PIPA) Authority: Personal Information Protection Commission (PIPC) and Korea Internet & Security Agency (KISA) Data breach notification time: Within 5 days if involving 1,000 or more data subjects
Spain	Regulation: GDPR (General Data Protection Regulation) and the Organic Law 3/2018 on the Protection of Personal Data and Guarantee of Digital Rights (LOPDGDD) Authority: Agencia Española de Protección de Datos (AEPD) Data breach notification time: Within 72 hours
Taiwan	Regulation: Personal Data Protection Act (PDPA) Authority: National Development Council (NDC), transitioning to Preparatory Division of the Personal Data Protection Commission (PDPC) Data breach notification time: Within 72 hours
United Kingdom	Regulation: UK GDPR and Data Protection Act 2018 Authority: Information Commissioner's Office (ICO) Data breach notification time: Within 72 hours
United States	Regulation: Varies by state; HIPAA, at federal level Authority: Varies by state; FTC, HHS at federal level Data breach notification time: Varies by state; generally without unreasonable delay, often within 30 days
Vietnam	Regulation: Decree No. 13/2023/ND-CP on Personal Data Protection Authority: Ministry of Public Security, Department of Cybersecurity and High-Tech Crime Prevention (AO5) Data breach notification time: Within 72 hours if high-risk breach
Republic of Ireland	Regulation: GDPR (General Data Protection Regulation) and Law No. 58/2019 Authority: Data Protection Commission (DPC) Data breach notification time: Within 72 hours

APPENDIX 2 : Privacy Definitions

Privacy Definitions	
Privacy Laws	Regulations designed to protect individuals' personal information and ensure their privacy rights. These laws govern the collection, use, storage, and sharing of personal data by organizations and government entities. They typically include provisions for data subject rights, such as the right to access, correct, and delete personal information, as well as requirements for data security and transparency in data processing. Privacy laws aim to balance the need for data utilization with the protection of individuals' privacy.
Privacy Authority	An independent public body responsible for overseeing the application of data protection laws. Privacy authorities have investigative and corrective powers to ensure compliance with privacy regulations. They provide expert advice on data protection issues, handle complaints related to privacy violations, and can enforce actions against organizations that breach data protection laws.
Data Subject	An individual whose personal data is collected, stored, or processed by an organization. Data subjects have specific rights regarding their personal information, including the right to access, correct, and delete their data, as well as the right to be informed about how their data is being used.
Data Controller	The person or entity (COP Group Companies) that determines the purposes and means of processing personal data. The data controller is responsible for ensuring that data processing complies with applicable laws and regulations.
Data Processor	The person or entity that processes personal data on behalf of the data controller. Data processors must follow the instructions of the data controller and comply with data protection laws.
Data Breach	An incident that leads to the unauthorized access, disclosure, alteration, or destruction of personal data. Data breaches can result in significant harm to individuals and require prompt action to mitigate risks.
Anonymized Data	Data that has been processed to remove or obscure personal identifiers, making it impossible to identify individuals from the data. Anonymization is intended to protect privacy by ensuring that data cannot be traced back to specific individuals.
Pseudonymized Data	Data that has been processed to replace personal identifiers with pseudonyms, which can be reversed to re-identify individuals if necessary. Pseudonymization enhances privacy while allowing data to be linked to the same individual across different datasets.
Data Subject Request	A request made by an individual to exercise their rights under data protection laws, such as accessing, correcting, or deleting their personal data. Organizations must respond to data subject requests within specified timeframes.
Data Processing Activities	Any operation or set of operations performed on personal data, whether or not by automated means.
Data Processing Agreement	An agreement between a data controller and a data processor that outlines the terms and conditions for processing personal data. This agreement ensures that data processing complies with legal requirements and protects individuals' privacy.

APPENDIX 3 Website, Cookies and Tracking Technologies

Third Parties links

Our website contain links to, or to be accessible from, websites provided by third parties. Your use of a Third Party Site will be subject to its terms of use and other provisions, and you are responsible for complying with such terms and provisions. Please note that this privacy policy does not cover the privacy policies or practices of any Third Party Site, and COP is not responsible for any information you submit to, or otherwise collected by, any Third Party Site. You should consult each Third Party Site for its privacy policy or practise before submitting any information to, or otherwise using, such Third Party Site.

Children

COP does not knowingly collect any information from children. Our site is not directed at children and should not be used by them. In no event should children provide any Personal data through our site. If the holder of parental responsibility of a child informs COP that the child's Personal data has been submitted to COP through the site without the parent's or guardian's consent, COP will use commercially reasonable efforts to remove such information from the Site and COP's servers at the parent's or guardian's request. To request the removal of Personal data of a child, the parent or guardian should contact COP as set forth in Section 12 and provide information necessary to COP to assist it in identifying the information to be removed.

Types of Cookies we Use

Our website uses cookies and similar tracking technologies to enhance your experience and analyse traffic. Cookies are small text files stored on your device that help us recognize you and remember your preferences.

- **Essential Cookies**: Necessary cookies help make a website usable by enabling basic functions like page navigation and access to secure areas of the website. They are essential for the proper function of the website.
- **Performance and Analytics Cookies**: Help the website owners to understand how visitors interact with websites by collecting and reporting information anonymously.
- **Functionality Cookies**: Allow our website to remember information that changes the way the website behaves or looks, like your preferred language or the region that you are in.
- **Targeting and Advertising Cookies**: Used to track visitors across websites. The intention is to display ads relevant and engaging for the individual user and thereby more valuable for publishers and third-party advertisers.

- **Unclassified Cookies**: Cookies that we are in the process of classifying, together with the providers of individual cookies.

Managing Your Cookies Preferences

You can manage your cookie preferences at any time through your browser settings. You can also opt-out of certain cookies by adjusting your settings on our Cookie Consent Tool. Please note that disabling certain cookies may affect your ability to use some features of our website.

COPENHAGEN OFFSHORE PARTNERS

APPENDIX 4 : Data Subject Request Form.

1. Contact Details

- **Full Name**:

2. Request Details

- **Type of Request** (Please select one or more):

☐ Access to Personal Data

☐ Rectification of Personal Data

☐ Erasure of Personal Data

☐ Restriction of Processing

☐ Data Portability

☐ Objection to Processing

☐ Withdrawal of Consent

- **Description of Request**:

_____

_____

_____

3. Verification of Identity

To successfully process your request, COP will need to verify your identity. In order to do so, COP's Compliance Team might contact you based on your selection below and ask you some questions based on the data we might already have from you, to corroborate your identity.

- **I would like to schedule:**

☐ An online meeting in the morning (Monday – Friday 09:00 – 12:00)

☐ An online meeting in the afternoon (Monday – Friday 13:00 – 17:00)

☐ A phone call in the morning (Monday – Friday 09:00 – 12:00)

☐ A phone call in the afternoon (Monday – Friday 13:00 – 17:0

Please, provide your e-mail or phone number based on the above selection.

Note: If you are submitting this form via our website [Copenhagen Offshore Partners | Contact], please copy this text to the message field.