As of mid-2018, personal data processing activities in EU member states will be governed by the General Data Protection Regulation (GDPR) and national specifications thereof, if and where these exist. One of the GDPR's key requirements is that personal data processing activities are made transparent to affected individuals.

Employers, who process personal data of their personnel for a variety of job-related purposes, are not exempted from this obligation. Therefore, this document provides BP staff in EU member states with the legally required information.

Please note, that this Statement does not cover systems/processes/applications which are available for your voluntary use. Information for each of those is provided directly to you prior to first use.

1. Who in BP is responsible for your employee data

The employing legal entity (which is party to your employment contract), is responsible for ensuring legally compliant handling of your personal data that it holds and processes in the context of your employment in accordance with BP’s global Data Privacy Policy.

Please contact your local HR adviser or, alternatively, the Local Privacy Coordinator in your country for any privacy related questions or concerns you may have. If you have questions before your first day at BP, please contact your recruiter.

2. Purposes, your personal data may be processed for

a) Fulfillment of legal and contractual obligations

From recruitment through to retirement employers have to fulfill a number of legal and contractual obligations arising from your employment. These may vary in line with the legal differences in national laws governing labor, tax, anti-discrimination, safety and security at work, etc. but will be well known obligations as listed below:

- Capturing worktime and absences (e.g. shift-planning, sick leaves, holidays, etc.)
- Role-related medical suitability checks
- Role-related capability checks (e.g. permit to work, driving license, etc.)
- Assurance of non-discriminating treatment and equal opportunities
- Training and development
- Payments (loans, salary, bonus, etc)
- Processing business expenses
- Tax payments and reports
- Other legal or regulatory reporting
- Accident/incident reports

b) Other purposes/processes in the legitimate interest of BP

Other processing activities may simply be justified by BP’s legitimate interest. Examples are:

- Control and optimization of BP’s overall organizational structure
- HR management reports, cost control and planning
- Succession planning for senior roles
- Data provision to support other business functions such as IT&S (Identity & Access Management), Finance (Delegation of Authority), Procurement, etc.
• Compliance checks with BP policies
• Evaluation of work performance (My Plan)
• Safety and security at work (incident management, evacuation trainings, video surveillance, etc.)
• Development and learning (My Talent & Learning)
• Office management (company badges, access to facilities, space planning, car parks, etc.)
• Social benefits (e.g. insurances, pensions, BP shares, fund matching, etc.)
• Support diversity goals / equal treatment
• Support for international assignments (e.g. immigration, relocation, etc.)
• Provision of business travel services (including visas etc.)
• Corporate credit card services
• Policy compliance checks, internal investigations of fraud or misconduct, grievance
• Maintenance of Ethics & Compliance registers

3. Occupational health services
Where BP offers occupational health services, any related health information (diagnosis, treatments, etc.) is kept by health professionals under duties of medical confidentiality and not shared with HR or any other party without your consent. For further details please refer to your local Health Team.

4. Categories of personal information processed
Categories of employees’ personal information BP may process in the employment context include:

• Personal details (name, home address, date and place of birth, bank-account no., marital status, next of kin, government issued identifiers, disability if any, etc.) Application data (CV, education, prior employers, skills, photograph, etc.)
• Interview notes (selection criteria, suitability/assessment details, etc.)
• Employment contract / details (role, salary grade, location, duration, etc.)
• Organisation classification data (segment, function, job, discipline, position)
• Compensation data including bonuses, allowances, equity, etc.
• Presence/absence periods including clocking and time records as required for payroll
• Business travel data (reasons, dates, bookings, expenditures)
• Performance details (MyPlan)
• Training data including course attendance and evaluations
• Potential, succession and career preferences information (My Profile)

Information about your racial or ethnic origin, physical or mental health, sex life, political or religious beliefs, biometric or genetic data, trade union memberships or criminal history will only be collected and processed, if we are legally obliged to or if you have provided your express and prior consent to do so.

5. Recipients of your personal information
Within the Group, your personal information will only be disclosed to authorized individuals if and to the extent necessary to fulfill a particular purpose. However, based on BP’s global matrix structure (into segments/functions/global businesses) teams in charge of particular tasks may not necessarily be located in your country of employment so that your data may be accessed from abroad. In any case, role-based access levels ensure that access to your personal data is limited on a strict need-to-know basis.

At BP, many processes/services are outsourced to external providers (e.g. global travel services, corporate credit cards, etc.). Whenever external parties are engaged to provide services which involve personal data (e.g. data hosting, application management and/or support, user support, etc.), these are carefully chosen. Their services are limited and clearly defined. Subject to written agreements which contain relevant legally required clauses on data protection. This ensures appropriately secure and confidential data handling (which is also limited to authorized staff only).
Sometimes, BP is legally obliged to disclose employees' personal information in response to a request from a court, tribunal or regulator, or as part of a litigation process. Where disclosure is in BP's discretion we will consult with you prior to making such disclosure and, in order to protect your privacy, we will only disclose the minimum amount of information necessary for the required purpose.

6. **Data transfers outside the EU/EEA or to international organizations**
BP group internal transfers of personal data outside the EU/EEA are legitimized by BP's Binding Corporate Rules. EU Data Protection Authorities have approved this framework in 2010, which guarantees an adequate level of data protection throughout the group.

If personal data is transferred outside the EU/EEA or to service providers which are internationally operating organizations, the recipients will either be contractually bound to a fixed set of data protection clauses as prescribed by European Commission or will have to be US-companies who self-certified to the Privacy Shield framework agreed between the EU and US. A copy of the data privacy relevant clauses agreed with a particular service provider can be made available on request.

7. **Data security**
The BP Group's global digital security standards are based on recognized international standards to protect systems and data against unauthorized access, damage, loss or destruction.

All staff, suppliers and business partners involved in the design, operation, management or use of digital technology, systems and information must comply with these security requirements. All access permissions granted to personal information held by BP Group companies is subject to strict security administration processes and must be limited to the business need.

To protect our information, BP's IT systems include suitable security measures to defend and detect any digital/cyber threats.

8. **Your rights related to your personal data**
Individuals in the EU are given a number of rights with regard to their own personal data including the right to lodge a complaint directly with a Data Protection Authority.

Applicable rights you can exercise are:
- **Access**: The right of access allows you to ask for a copy of your personal data.
- **Rectification**: This right allows you to request any false personal data to be corrected or incomplete data to be amended.
- **Restriction**: This right allows to stop/suspend the further processing of personal data e.g. until a dispute is resolved.
- **Erasure**: You can request the deletion of personal data, which is not processed in compliance with privacy legislation (e.g. illegally obtained data or where the justified data retention period was exceeded).

9. **Data retention periods**
Unless e.g. labor, tax or other applicable laws require BP to retain certain information for a specified minimum period of time, your personal information will be retained in line with BP "Records Retention Schedule" or otherwise only as long as necessary to fulfill the particular purpose.

After that time your data will be either deleted or de-personalized, e.g. if used for long-term statistical purposes.

- END -