Data Privacy Rules Public Document

DOCUMENT NAME & LOCATION:	Data Privacy Rules Public Document
DOCUMENT VERSION:	2.0
DATE:	13-January-17
READERSHIP:	Public
SUMMARY:	This document outlines BP's 16 Data Privacy Rules and how individuals can contact BP in relation to their personal information.

Contents

Part I – Background

Introduction

Since 2001 BP has had a Data Privacy Policy articulating global standards with respect to data privacy compliance. In 2010 BP gained approval for its Binding Corporate Rules from the UK Information Commissioner's Office. BP's Binding Corporate Rules are the global compliance framework used within the company to manage and process personal information. The 16 data privacy rules stated in this document are also in the internal BP Data Privacy Policy. These rules, along with other internal practical procedures, comprise the privacy compliance framework known as BP Binding Corporate Rules ("BCR").

The BCR are binding on BP p.l.c. and its specifically nominated entities (referred to in this document as the "**BP Entities**", "**we**" **or** "**us**"). All these BP Entities are under a legal duty to respect and comply with the BCR. The BCR apply to all personal information used and collected of any employees, contractors, customers and business contacts of the BP Entities, as well as any other categories of individuals about whom BP may process personal data.

The BP Entities are more recognisable by the various BP brands and a brief overview of BP brands (as at January 2017) is given below:

- **BP** is our main global brand. It is the name that appears on production platforms, refineries, ships and corporate offices as well as on wind farms, research facilities and at retail service stations
- **Castrol** the lubricants brand was acquired by BP in 2002. Castrol's motor oils for automobiles and motorbikes are particularly well known. But Castrol also makes lubricants for every conceivable application on land, sea and in the air. Castrol products are sold in more than 150 countries
- **Aral** is one of the most trusted brands in Germany. It has been associated with quality automotive fuels since the 1920s. Today people also associate Aral with good food and excellent service 'on the go'
- The first **ampm** shop opened in California in 1978. There are now more than 900 of them situated within Arco service stations in the western United States
- **Wild Bean Cafe** is part of many BP Connect petrol stations. These 'on the go' cafés are found in parts of Europe, Australasia and South Africa. We also have a presence in China and Russia, and new branches are opening all the time.

The purpose of this document is to explain:

- the data privacy rules
- your rights/privileges under the BCR
- what to do if you have a query or a complaint
- how to contact us

What is data protection law?

Data protection laws allow people to manage how their personal information (any information that relates to them, such as a name, identification numbers, photos, preferences, employment records, etc.) is used. BP's use of the personal information of its employees, contractors, customers, business contacts or any other identifiable individuals is covered and regulated in many cases by local data protection law, or if no laws exist then BP's Data Privacy Policy.

How do data protection laws affect BP Entities internationally?

European data protection laws do not allow the transfer of personal information to countries outside the European Economic Area (EEA) that do not ensure an 'adequate' level of data protection. Many of the countries in which the BP Entities operate are not regarded by the EEA as providing an adequate level of data protection and/or privacy.

Applying European data protection standards across the BP Entities by means of the BCR is how BP has decided to ensure that an adequate level of protection exists for transfers of personal information across BP's international operations.

How are we doing that?

The BCR are based on European data protection standards and comprise the rules and internal practical procedures with respect to data privacy compliance. The rules must be followed by each employee and contractor of BP Entities when handling personal information and, if there are any local laws that substantially affect the ability of the BP Entities to comply with the BCR, of which the BP Entities are aware, those BP Entities must tell their local privacy coordinator and/or regional privacy adviser who will consult with the data protection supervisory authority with competent jurisdiction to determine an appropriate course of action.

Applying European data protection standards across the BP Entities by means of the data privacy rules is the best way for the BP Entities to ensure that an adequate level of protection exists for transfers of personal information across the BP Entities' international operations.

Compliance with the BCR forms part of our regular awareness and training around Data Privacy. In addition, regular audits will be carried out to assess whether the BCR are being adhered to in practice. We will take appropriate steps to deal with any instances of non-compliance.

This document contains the 16 data privacy rules contained in the BCR adopted by BP. The BP Data Privacy Policy contains further detailed guidance to assist employees and contractors who work with personal information to put the rules into practice.

These data privacy rules will be construed in accordance with and governed by the laws of England and Wales.

Part II – The rules

Rule 1 – We shall first and foremost comply with local law where it exists.

As an organisation BP must always comply with any applicable legislation relating to personal data (e.g. in the United Kingdom, the Data Protection Act 1998). In some countries there may be state laws that apply as well as federal laws, and there may be ancillary administrative regulation in addition to legislation.

Where there is no law or the law does not meet the standards set out by the rules in this document, we will process personal information in adherence to the rules in this document. We must be aware of any local or regional laws affecting the use of personal data and never ignore them.

Rule 2 – We shall ensure that BP representatives take ownership of data protection.

The global privacy lead will ensure that the business leadership in each BP country where we have more than 20 employees nominates an individual as a local privacy coordinator who will be responsible for overseeing compliance with national and regional law and the rules outlined in this document. Any data privacy matters of material risk must be referred by the local privacy coordinator to a regional privacy adviser in the central data privacy team which has overall responsibility for ensuring compliance with the BCR.

Rule 3 – We shall honour our commitment to each other as a global organisation.

BP has made a public decision to adopt and abide by these rules. This commitment is our responsibility and must be honoured by all.

All individuals who manage personal data within the BP Entities should be aware of these rules and the commitment we have made to follow them.

Rule 4 – We shall be open with individuals as to how their personal information will be used by us.

Being open and transparent in the way we use and share our employees', contractors', customers' and business contacts' personal information is the most important step we can take to create good privacy practices. We must ensure that individuals are always told in a clear and comprehensive way about the uses, disclosures and other processing activities performed on their information when such information is obtained. If it is not practicable to give notice at the point of collection, then notice should be given as soon as possible thereafter. There may be legitimate reasons for not providing notice in limited cases, for example, where it is necessary to safeguard national security or defence, for the prevention or detection of crime, taxation purposes, legal proceedings or where otherwise permitted by law.

Rule 5 – We shall only obtain and use personal information for those purposes which are known to individuals or which are within their expectations and are relevant to us.

When collecting personal information from individuals, we will ensure that the privacy statement made available to those individuals contains all of the purposes for which the personal information may be used as described by Rule 4. In addition, when collecting information, we will only collect those details which are necessary for the purposes for which that information is being obtained.

Rule 6 – We should only change the purpose for which personal information is used if we make people aware of such change or it is within their expectations and they can express their concerns.

If personal information is collected by the BP Entities for a specific purpose (as communicated to the individual via the relevant privacy statement or policy) and subsequently any of the BP Entities wish to use the information for a different or new purpose, we will ensure that the relevant individuals are aware of such a change unless there are legitimate reasons for not having to do so as described in Rule 4. In certain cases, the individual's consent to the new processing activities may be necessary.

Rule 7 – We shall keep personal information accurate and up to date.

Processing inaccurate information can be harmful to individuals and to the business. The main way of ensuring that personal information is kept accurate and up to date is by actively encouraging employees, contractors, customers and business contacts to inform us when their personal information changes.

Rule 8 – We shall keep personal information only for as long as is really necessary.

Any personal information relating to individuals should only be kept where there is a business or legal need to do so.

Policies for the destruction of obsolete data will be devised and implemented at departmental level in each country in which the BP Entities operate.

Rule 9 – We shall always be receptive to any queries, requests or complaints made by individuals in connection with their personal information and adhere to our Access Request Response Procedure.

We recognise that individuals should have the ability to access personal information held about them. Individuals are entitled (by making a request to the relevant BP Entity) to be supplied with a copy of any personal information held about them (including both electronic and paper records) unless there is a legitimate basis for withholding the information.

If a valid request concerns a change in that individual's personal information, such information must be rectified or updated, if appropriate to do so.

We will reply to queries and complaints in reasonable time and to the extent reasonably possible concerning the processing of personal information by the BP Entities.

Rule 10 — We shall always adhere to appropriate technical and organisational security measures to protect personal information.

Personal information must be kept secure. Technical and organisational security measures are necessary to prevent the unauthorised or unlawful processing or disclosure of personal information, and the accidental loss, destruction of, or damage to, personal information.

We will:

- Assess the level of security applied to a set of information, taking into account current standards and practices.
- In particular, we will observe our internal security standards in this regard.

Rule 11 – We shall ensure that providers of services to us also adopt appropriate and equivalent security measures.

Where a provider of a service to the BP Entities has access to our employees', contractors', customers' and business contacts' personal information, we must impose contractual obligations dealing with the security of that information.

All contracts with providers of such services should therefore include appropriate contractual provisions.

Rule 12 – We shall never transfer personal information to non-BP Entities without ensuring that the third parties provide the right level of protection.

Transfers of personal information to countries outside the European Economic Area that do not ensure an 'adequate' level of data protection and all other transfers of personal information within the BP Entities will be covered by these rules. However, international transfers of personal information outside BP Entities are not allowed without appropriate steps being taken, such as contractual clauses which will protect the personal data being transferred. Therefore, we must always abide by these rules and we must not transfer any personal information to non-BP Entities companies or individuals outside the European Economic Area, without taking these appropriate steps.

Rule 13 – We shall only use sensitive personal information if it is absolutely necessary for us to use it.

Sensitive personal information is information relating to an individual's racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, health, sex life and criminal convictions. This information deserves more stringent protection than other personal information so our standards of care must be higher when dealing with this type of information. We must always assess whether sensitive personal information is essential for the proposed use and only collect sensitive personal information when it is absolutely necessary in the context of our business.

Rule 14 – We shall only use sensitive personal information where we have obtained the individual's explicit consent unless we have another lawful basis for doing so under European data protection law.

Given the nature of this type of information, (which includes information relating to health, religion or ethnic origins) it is only appropriate for us to collect and use sensitive personal information when people explicitly agree or where there in another lawful basis for doing so under European data protection law. Where explicit consent is being relied upon, this permission to our use of sensitive personal information must be genuine and freely given.

Rule 15 – We shall always allow customers to opt out of receiving marketing information.

One of the key data protection elements is that individuals have the right to object to the use of their personal information for direct marketing purposes and BP Entities must honour all such opt out requests.

We must ensure that the data protection statement made available when personal information is collected includes the relevant opt out mechanisms regarding marketing communications.

Rule 16 – We shall always suppress from marketing initiatives the personal data of individuals who have opted out of receiving marketing information.

It is essential that customers' choices are accurately identified when direct marketing campaigns are carried out.

Those responsible for a direct marketing campaign must take all necessary steps to prevent the sending of marketing materials to individuals who have opted out.

Part III – Our commitment to individuals

One of the requirements of the EEA data protection law where personal information is transferred from a BP Entity within the EEA to a BP Entity outside the EEA is that the individuals whose personal information is transferred must be able to benefit from certain rights in respect of that information. As a result, our customers, employees, contractors and business contacts whose personal information is transferred from a BP Entity within the EEA to BP Entities outside the EEA will be able to benefit from the following rights:

- to be informed about the uses and disclosures made of the information;
- to be able to obtain a copy of the Data Privacy Rules Public Document on request;
- to receive a copy of the deed poll entered into by the BP Entities, the Data Privacy Rules and any of the relevant practical procedures as may be required to enforce their rights under the BCR through a data protection authority based in the EEA of competent jurisdiction or through a court of competent jurisdiction if a complaint cannot be resolved through the BP complaints procedure;
- to be replied to in a reasonable time and to the extent reasonably possible about queries concerning the processing of their personal information by the BP Entities;
- to make complaints, obtain appropriate redress and, where appropriate, receive compensation for any damage suffered as a result of a breach by the BP Entities of the terms set out in the BCR;
- to lodge a complaint with an EEA data protection authority with competent jurisdiction and/or to take action through a court to enforce compliance by the BP Entities with all applicable principles, rules and practical procedures set out in the BCR.

These rights will only apply to personal information transferred in the circumstances described above.

It is BP's aim to try to deal with any complaints arising in connection with the BCR as quickly as possible and the complaints procedure is set out in Part IV below.

Part IV – Complaints procedure

Employees

If you have any complaint about the way in which your personal information has been handled under the BCR, you may raise the matter with your immediate line manager. If your complaint relates to your immediate line manager, or is something which does not relate to your immediate work area, you may raise the matter with either the appropriate HR representative or the next level of leadership (above your immediate line manager). Complaints should be made in writing and copied to an appropriate HR representative. You may also contact the Central Data Privacy Team at **privacy3@bp.com**.

Non-Employees

BP is committed to protecting personal data and takes any complaint seriously and ensures it is dealt with fairly and effectively. There are a number of ways that you can register a complaint:

You can identify a contact within BP using the BP.com website (www.bp.com). See the "contact us" section on the home page and you will be able to navigate to the appropriate contact information for a specific country. Where your complaint is in relation to a specific data privacy issue, the BP privacy statement is located at the bottom of each BP website page with the e-mail contact address (**privacy3@bp.com**) contained within it. You can contact the central data privacy team on a specific data privacy issue directly by using this address remembering to clearly state the following:

- The specific data privacy complaint (please provide as much detail as possible including country, BP company/ brand, your understanding of the data privacy infringement and issues, redress requested);
- Your full name and how we can contact you;
- Any previous correspondence on this specific data privacy issue.

Procedure for handling complaints

Your complaint will be forwarded to the local privacy coordinator (or privacy officer) and, if necessary, forwarded to the regional privacy advisers within the central data privacy team. In the majority of cases, complaints will be dealt with locally.

We aim to resolve all issues in a timely manner, or as mandated by local law, but if this is not possible because a more detailed investigation is required, we will keep in regular contact with you to ensure that you are kept informed of the resolution of your matter.

If you are not satisfied with the way in which your complaint has been dealt with, you have the right to lodge a complaint with an EEA data protection authority with competent jurisdiction and/or to take action through a court to enforce your rights under the BCR in the jurisdiction of the BP Entity responsible for exporting the information from the EEA. This is because under the BCR claims may be made against the BP Entity responsible for exporting the information even where the alleged breach is as a result of the actions of the importing BP Entity. If you wish to make a claim against BP as a result of an alleged breach of the BCR that may result in compensation being payable, if you can establish facts which show that it is likely that the damage has occurred because of the breach of the BCR by one or more of the BP Entities, the BP Entity responsible for exporting the personal information from the EEA under the BCR will accept the burden of proof to demonstrate that liability for any breach of the BCR which has resulted in the claim for compensation does not rest with the BP Entity or Entities which are the subject of the claim.

Part V– Data protection authority cooperation mechanism

We have agreed to cooperate with the EEA data protection authorities as follows:

- by making the necessary personnel available for dialogue with the EEA data protection authorities who have competent jurisdiction where required;
- by actively reviewing and considering any decisions made by any EEA data protection authorities who have competent jurisdiction on data protection law issues that may affect the BCR, and the views of the Article 29 Working Party as outlined in its published guidance on BCR;
- by providing copies of the results of any BCR audit to a relevant national EEA data protection authority with competent jurisdiction upon request subject to applicable law and respect for the confidentiality and trade secrets of the information provided;
- by accepting that any relevant national EEA data protection authority with competent jurisdiction may audit any BP company within its jurisdiction which is covered by the BCR for the purpose of reviewing compliance with the BCR subject to applicable law with full respect to the confidentiality of the information obtained and to the trade secrets of BP;
- by agreeing to abide by a formal decision of the applicable EEA data protection authority with competent jurisdiction which is final and against which no further appeal is possible on any issues related to the interpretation and application of the BCR, and;
- by communicating any material changes to the BCR to the UK Information Commissioner's Office and/or any other EEA data protection authority with competent jurisdiction at least once a year together with an explanation for those changes (save for changes which are administrative in nature or have occurred as a result of a change of

applicable data protection law in any EEA country, through any legislative, court or supervisory authority measure).

Part VI – Changes to the BCR

In the event that the terms of the BCR vary, this document will be amended to reflect those changes and will state the date on which the BCR was last reviewed and also the date on which any revisions were made.

Effective date:	31 March, 2010
Date BCR last reviewed:	13 January, 2017
Date BCR last revised:	13 January, 2017
Department:	BP Legal
Responsibility:	Global privacy lead

Want more information?

If you have any questions regarding the BCR, how to exercise your rights, or any other data privacy issues, please contact our global privacy lead at: privacy3@bp.com.