GLOBAL DATA PROTECTION POLICY

Document Approved by: DP World Group Board
Policy Owner: Group Compliance
Revision Number: 4
Revision Date: April 2025

TABLE OF CONTENTS

INTRODUCTION

DP World, including all DP World entities, subsidiaries and business units (**"DP World"**) is committed to complying with data protection laws, in all of the jurisdictions that it operates in, including but not limited to the General Data Protection Regulation 2016 ("GDPR"), the UK GDPR, the South African Protection of Personal Information Act 4 of 2013 ("POPIA"), the UAE Federal Decree-Law No. 45 of 2021, and California's Consumer Privacy Act ("CCPA"). The protection of personal data is the responsibility of all of us. As such, DP World asks all readers to abide by the guidelines as set out in this policy.

Terms used in this policy which are underlined and in bold (e.g. **personal data**) are defined in Definitions and Terms at the end of the policy (paragraph 15 below).

In the course of its business, DP World needs to process **personal data** about individuals. This includes, but is not limited to:

- collecting information from prospective, current, and former employees;
- managing employee information;
- collecting and managing information from prospective, current, and former customers;
- providing the provision of services; and
- contracting with third parties to process data on behalf of DP World.

The collection, handling and storage of personal data is regulated by law in many jurisdictions. DP World is committed to putting organizational and technical measures in place to comply with its legal and regulatory obligations.

PURPOSE, SCOPE, AND CONTACT INFORMATION

While our principles at DP World emphasize the continued growth of our business, DP World never seeks to grow its business in a way that is unethical, unlawful or creates hidden risks.

This policy sets out principles to be followed by staff and other stakeholders in relation to the processing of personal data in the course of their employment by, or interaction with DP World.
DP World takes compliance with all applicable data protection laws seriously. Violations of data privacy laws may result in significant fines, reputational damage, and penalties not only for DP World, but for any individuals involved in the misconduct. Such individuals may also face disciplinary action, including termination.

This policy may be supplemented by additional documents, designed to ensure compliance with the further requirements of data protection laws in particular jurisdictions.

This Policy applies to all DP World directors, officers, authorized representatives, and employees ("Staff") and any third-party conducting business on DP World's behalf, including, but not limited to, joint venture partners, agents, consultants, suppliers, vendors, and/or other third-party representatives ("Other Stakeholders").

While this Policy sets forth certain mandatory standards, it does not address every situation in relation to processing personal data. Accordingly, it is the responsibility of everyone at DP World, including anyone working on its behalf, to always ensure compliance with legal and regulatory obligations, conduct themselves in an ethical manner and exercise good judgment, in accordance with DP World's global standards and expectations. If you have any questions about this Policy or uncertainty about whether a business activity or transaction is permitted by this Policy and/or applicable law, we encourage you to contact your supervisors, or, if you prefer, Group Compliance through the channels detailed in this Policy.

All queries in relation to this policy should be directed to your regional Group Compliance team and/or the Group Compliance e-mail (groupcompliance@dpworld.com).

DATA PROTECTION REPRESENTATIVE

DP World has nominated data protection representatives ("DPRs") in the following Regions:

- Africa
- Americas
- Asia
- Europe
- Middle East
- Russia

A Data Protection Officer (DPO) (or a similar naming convention as described in the relevant jurisdiction) is designated where legislation requires them and the contact details of each DPO will be published as necessary.

DP World also has a Group DPO, who is responsible for data protection and privacy on an entire Group, and therefore Global basis.

There will be Privacy Custodians in each business unit, as required, who will assist the Compliance Team with data protection and privacy matters.

DP World will ensure that business units that are subject to the extra territorial provisions of a relevant data protection/privacy law, will, where that data protection/privacy law requires, designate in writing a representative located in the applicable country.

TRANSPARENCY

Where DP World processes personal data about data subjects, it should, at the time when personal data is obtained, provide the data subject with information necessary (through the form of a privacy notice) to ensure that the processing is fair and transparent, including:

- DP World's identity and contact details;
- the contact details of the DPR/DPO or Representative (in accordance with clause 3.2 above) as applicable;
- the purposes of the processing for which the personal data is intended, as well as the legal basis for the processing;
- the categories of personal data concerned;
- the recipients or categories of recipients of the personal data, if any;
- if applicable, the fact that DP World intends to transfer the personal data to a third country or international organization, a reference to the safeguards it has put in place in this respect and how to obtain a copy of them, or where they have been made available – please see paragraph 7 below;
- the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- the existence of data subject rights, including access, rectification or erasure of personal data, restriction of processing or objection to processing, right to withdraw consent (where applicable), and the right to lodge a complaint with a supervisory authority; and
- the source from which the personal data originates, and if applicable, whether it came from publicly accessible sources.

Such information is usually provided by the relevant DP World privacy notices, which have been designed to contain all relevant information. DP World has one employee privacy notice and four external privacy notices. Please refer to the applicable privacy notice whenever possible.

LEGITIMACY AND FAIRNESS OF PROCESSING

DP World will only process personal data fairly, lawfully, and in a transparent manner (lawfulness, fairness and transparency). In particular:

- it will only collect and process personal data for specified, explicit, and legitimate purposes (these may be business, regulatory, compliance or other purposes) and not further process the personal data in a manner that is incompatible with those purposes ('purpose limitation');
- it shall not process personal data, which is irrelevant, excessive or inadequate, given the purposes for which those personal data is collected and processed ('data minimization');
- it will take reasonable steps to ensure that data is accurate and, where necessary, kept up to date; it shall also take reasonable steps to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, erased or rectified without delay ('accuracy');
- it shall ensure that personal data is kept no longer than is necessary ('storage limitation');
- it shall ensure appropriate security measures are in place in respect of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality'); and
- it shall be responsible for, and be able to demonstrate compliance with this paragraph 5 ("accountability").

SENSITIVE PERSONAL DATA

DP World shall not process sensitive personal data, except where explicitly allowed to do so, and ensure that it is done in compliance with all applicable data protection laws.

DATA TRANSFERS

DP World shall not disclose personal data to anyone, including within DP World, except in the following circumstances:

- within DP World where the recipient of the personal data needs such data for a legitimate business, HR or compliance purpose;

- within or outside DP World, subject to compliance with the outsourcing rules in paragraph 11.3 below; and

- where authorized by a DPR on the basis that such disclosure complies with applicable data protection law.

AUTOMATED DECISION-TAKING AND PROFILING

Apart from in the recruitment process, DP World will not use automated decision-taking techniques or profiling unless after prior consultation with a DPR.

RESPECT FOR INDIVIDUALS' RIGHTS

The DPRs should immediately be notified when a data subject asks a question about the processing of his/her personal data. If you receive a communication from any data subject in which he or she seeks to exercise rights of access to, rectification or erasure of, or restriction or objection to the processing of personal data held by DP World or withdrawal of consent or data portability, that communication should be promptly passed to a DPR, so that DP World can respond appropriately within the deadline under the applicable data protection law.

RECORDS OF PROCESSING ACTIVITIES (ROPA)

DP World shall maintain a record of processing activities that contains all of the following information:

- the name and contact details for DP World (including the relevant DP Group entity);

- the purposes of the processing;

- a description of the categories of data subjects and of the categories of personal data;

- the categories of recipients to whom the personal data has been or will be disclosed, including recipients in third countries or international organizations;

- where applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization and, if applicable, the documentation of suitable safeguards;

- where possible, the envisaged time limits for erasing different categories of data; and

- where possible, a general description of the relevant technical and organizational security measures put in place to protect personal data.

DATA SECURITY

All DP World entities will have in place appropriate technical and organizational measures, and follow data security policies designed to ensure that personal data is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures, and against all processing which is in breach of this policy or otherwise unlawful. The level of data security ensured by these policies must be appropriate to the nature of the personal data protected and the risks associated with their processing, but, considering the security measures available and their cost. These measures should be respected and complied with at all times.

In this respect, DP World will implement, where appropriate, the following measures to ensure a level of security appropriate to the risk:

- pseudonymization and encryption;
- ensuring confidentiality, integrity, availability and resilience of processing systems and services;
- ability to restore availability and access to personal data in a timely manner in the event of an incident; and
- the regular testing and evaluating of technical and organizational measures designed to ensure security of data processing.

Where DP World outsources the processing of personal data to any service provider it shall:

- conduct appropriate due diligence on the technical and organizational security arrangements that the service provider will have in place to protect personal data;
- ensure that the arrangement is governed by a written agreement meeting the requirements of applicable data protection laws, requiring the service provider to process such personal data only on DP World's documented instructions and to have appropriate technical and organizational security measures in place to protect the personal data against unauthorized or unlawful processing and accidental loss, destruction or damage; and
- take reasonable steps (for example, by making enquiries of the service provider or exercising

audit rights) to ensure that those security measures in place are in practice.

DATA BREACHES

All actual or potential data protection compliance failures must be reported to a DPR without delay and as soon as reasonably practicable so that the DP World can respond appropriately and in accordance with the applicable law.

Any suspected or detected breach, loss or other risk situation that could lead to a data breach, should be notified to a DPR immediately. It should be taken into account that DP World may be bound to notify the competent authorities of breaches within a required period of time.

DATA PROTECTION IMPACT ASSESSMENT

Where a new process or system involving the processing of personal data is to be implemented within or on behalf of DP World, in particular using new technologies, or a material change is to be made to an existing process or system, the initiative/business owner responsible for the implementation of or change to the process/system, should first assess the impact of the envisaged processing operations on the protection of personal data.

When carrying out a data protection impact assessment, the DP World data protection impact assessment template should be used.

RETENTION

DP World will delete or anonymize personal data when it is no longer necessary for the purposes for which the personal data was originally processed, taking into account DP World's business, HR, compliance, legal and other reasons to retain personal data and the need to retain and delete personal data in accordance with DP World's retention policy and schedule.

DEFINITIONS AND TERMS

automated decision-taking techniques means making decisions legally or significantly affecting individuals on the basis of the automated processing of personal data relating to them, without human intervention (for example, the pre-screening of employment applications);

data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed;

data subject means an individual (for example, an employee of DP World or of a supplier, customer, other business partner or regulator of DP World) to whom personal data relates;

personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; Examples of personal data include email addresses, phone numbers, IP addresses, unique reference numbers and ZIP code;

Privacy Custodians means a network of DP World employees that champion data protection and privacy within DP World, and help assist Group Compliance implement data protection and privacy best practice across the various businesses;

processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means (therefore this includes manual filling as well); essentially processing has a very wide definition;

profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements;

pseudonymization means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

sensitive personal data means personal data consisting of information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation (or any personal data that is described as sensitive personal data under applicable data protection laws).

REPORTING REQUIREMENTS

If you become aware of any issue or practice that may constitute a potential violation of applicable law, any provision outlined in this Policy, or any other DP World Policy, it is your responsibility to promptly report the matter as outlined below. For example, if you receive a request or demand around personal data that involves providing or selling personal data ,

and such a request is related to a breach of this Policy, you must immediately reject the demand and report the issue. When refusing, keep in mind the following:

- explain that making the payment would violate this Policy, DP World's Code of Ethics, and anti-corruption laws;
- make it clear that the refusal is absolute; and
- if any other stakeholder is involved, clearly explain that they are not authorized to make an improper payment on behalf of DP World or DP World will terminate their contract and may report the other stakeholder to the relevant governmental authorities if any such a payment is made.

All **queries** in relation to this policy should be directed to your regional Group Compliance team and/or the Group Compliance e-mail (groupcompliance@dpworld.com).

All concerns in relation to any these policy violations to be reported in accordance with Group Whistleblowing Policy through the following channels:

Whistleblowing Hotline:

- Online - external: www.dpworld.com/whistleblowing-hotline;
- Online - company intranet: See DP World Connexions or business unit intranet as applicable; and/or
- Telephone: Freephone number as publicized on intranet, websites, and within DP World premises in each country of operations.

All reports will be taken seriously. A prompt investigation will be initiated following any credible indication that a breach of this Policy or applicable Anti-bribery laws has occurred. Appropriate corrective action will be taken, as necessary. The specific action taken in any particular case depends on the nature and gravity of the conduct or circumstances reported.

DP WORLD STRONGLY AND STRICTLY PROHIBITS RETALIATION AGAINST ANYONE WHO, IN GOOD FAITH, RAISES A CONCERN ABOUT A POSSIBLE VIOLATION OF APPLICABLE LAW, DP WORLD'S CODE OR ANY DP WORLD POLICY. ANY ACT OR THREAT OF RETALIATION WILL ITSELF BE CONSIDERED A SERIOUS VIOLATION OF DP WORLD'S CODE OF ETHICS.

ANY SUSPECTED OR OBSERVED ACTS OF RETALIATION SHOULD BE IMMEDIATELY REPORTED.

AWARENESS AND TRAINING

Training, will be provided via business units and Group Compliance during the new employee onboarding process (and will be refreshed on a regular basis). Supplemental targeted training will be provided to select employees thereafter, as appropriate, on a periodic basis, as determined by the Group Sr. VP – Compliance. Group Compliance will maintain records of training materials, and the relevant Business Unit, Regional, Divisional People functions will maintain records of DP World Employee attendance at training sessions.

TESTING AND AUDIT

DP World, through its compliance function and supported by other relevant functions, will perform risk-based testing of its data protection compliance program on a periodic basis, working with business units, Privacy Custodians and data protection teams. The testing should be performed by individuals who are not responsible for the day-to-day operation of data protection. The results of such independent testing will be reported to the Group Sr. VP -Compliance, senior management, and/or the Board of Directors.

REVISION HISTORY

VERSION NUMBER	UPDATE DETAILS	APPROVAL DATE
4	INTERNAL REVIEW AND UPDATED TO ENSURE DOCUMENT IS FIT FOR PURPOSE ON A GLOBAL BASIS	APRIL 2025
3	REVIEW LINKLATERS	10 MAY 2018
2	UPDATED FOR EU GDPR	
1	INITIAL DRAFT – DPA 1998	04 FEB 2014