Data Protection policy

1. Purpose

This policy sets out how the CIPD Group ('we', 'our', 'CIPD') handles Personal Data of our customers, suppliers, employees, workers, volunteers and other third parties. The CIPD Group comprises:

- The Chartered Institute of Personnel and Development (including CIPD Ireland)
- CIPD Enterprises Ltd
- CIPD Asia Ltd
- CIPD Middle East FZ-LLC

(Each organisation in the CIPD Group is a Data Controller and where UK based, the Information Commissioner's Office ('ICO') is the supervisory authority.)

This policy is our internal document and must not be shared externally without prior authorisation from our Head of Legal. It is intended to ensure that CIPD complies with GDPR in relation to all Personal Data that we process regardless of the media on which that data is stored or whether it relates to past or present employees (including job applicants), workers, volunteers, customers (including members), clients or supplier contacts or website users. (*Glossary of capitalised words is set out in the appendix*.)

2. Scope and Responsibilities

Protecting Personal Data is a critical responsibility that we take seriously at all times. CIPD is exposed to potential fines of up to EUR20 million or 4% of total worldwide annual turnover, whichever is higher for failure to comply with the provisions of GDPR.

This policy applies to all CIPD People ('you', 'your'). You must read, understand and comply with this policy when Processing Personal Data on our behalf and attend training on its requirements. This policy sets out what we expect from you in order for CIPD to comply with applicable law. Your compliance is mandatory and any breach of this policy shall be subject to investigation and may result in disciplinary action.

All team managers are responsible for ensuring their teams implement appropriate practices, processes, controls and undertake training (including CIPD's mandatory training) to ensure compliance with this policy.

Our Legal and Governance Director is responsible for reviewing and updating this policy. Please check Workspace to obtain the latest copy of this policy.

If you have any questions about this policy or any of the processes and policies referred to within it please contact our Legal and Governance Director or the legal team.

3. Data Protection Principles

CIPD adhere to the principles relating to Processing of Personal Data set out in GDPR which require Personal data to be:

(a) Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency).

(b) Collected only for specified, explicit and legitimate purposes (Purpose Limitation).

(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation).

(d) Accurate and where necessary kept up to date (Accuracy).

(e) Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation).

(f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality).

(g) Not transferred to another country without appropriate safeguards being in place (Transfer Limitation).

(h) Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

(a) Lawfulness, Fairness and Transparency

Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. This means, you must tell the data subject what Processing will occur (transparency); the Processing must match the description given to the Data Subject (fairness), and it must be for one of the purposes specified in GDPR (lawfulness).

Lawfulness GDPR restricts our actions regarding personal data to specified lawful purposes. These restrictions are not intended to prevent processing, but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

GDPR allows Processing for specific purposes, those most relevant to CIPD are set out below:

- the data subject has given his or her Consent (see *Consent* section below);
- the Processing is necessary for the performance of a contract with the Data Subject;
- to meet our legal compliance obligations; or

- to pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we Process Personal Data for legitimate interests must be set out in our Privacy Policy.

You must identify and document the legal ground being relied on for each new processing activity.

Consent

A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly, either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

Data Subjects must be easily able to withdraw consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

Unless we can rely on another legal basis of Processing, Explicit Consent is usually required for Automated Decision-Making and for cross border data transfers.

CIPD will only Process Special Categories of Data where the Data Subject has given explicit Consent to such Processing or where one of the following conditions applies:

- the Processing relates to Personal Data which has already been made public by the Data Subject.

- the Processing is necessary for the establishment, exercise or defence of legal claims.

- the Processing is specifically authorised or required by law.

- the Processing is necessary to protect the vital interests of the Data Subject or of another person where the Data Subject is physically or legally incapable of giving consent.

When relying on Consent to Process Data, you will need to evidence the Consent captured and keep records of all Consents so that CIPD can demonstrate compliance with GDPR.

In any situation where new Special Categories of Data are to be Processed, you must inform our Head of Legal who will record the basis for the Processing together with the Personal Data in question on CIPD's data processing register.

Transparency GDPR requires Data Controllers to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. Data Subjects must be made aware of the purpose for which their Data is collected and how it will be used. CIPD will provide such information through an appropriate Privacy Policy on its website. You must provide a copy of the Privacy Policy to the Data Subject at the time of data collection.

Information provided to the Data Subject must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand it.

When Personal Data is collected indirectly (for example, from a third party or publically available source), you must provide the Data Subject with all the information required by GDPR as soon as possible after collecting/receiving the Data. You must also check that the Personal Data was collected by the third party in accordance with GDPR and on a basis which contemplates our proposed Processing of that Personal Data.

(b) Purpose Limitation

Personal Data shall be collected for specified, explicit and legitimate purposes. It must not be further Processed in a manner that is new, different or incompatible with these purposes unless you have informed the Data Subject of the new purposes and they have Consented where necessary.

This means you must specify exactly what the Personal Data collected will be used for and limit the Processing of that Personal Data to only what is necessary to meet the specified purpose.

(c) Data Minimisation

Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

This means you may only collect and Process Personal Data required for your job: do not collect excessive Data. Ensure any Personal Data collected is adequate and relevant for the intended purposes.

You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with *CIPD's data retention policy*.

(d) Accuracy

Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

This means you must ensure that the Personal Data you use and hold is accurate, complete, kept up to date and relevant to the purpose for which you collected it. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

(e) Storage Limitation

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the Personal Data is Processed.

This means you must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements. You must comply with *CIPD's data retention policy* and take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require. This includes requiring third parties to delete such Data where applicable.

(f) Security, Integrity & Confidentiality

Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

Protecting Personal Data We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks (including use of encryption and Pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data.

You are responsible for protecting the Personal Data you Process. You must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. You must exercise particular care in protecting Special Categories of Personal Data from loss and unauthorised access, use or disclosure. You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

- Confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it.

- Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed.

- Availability means that authorised users are able to access the Personal Data when they need it for authorised purposes.

You must comply with our *Information Security Framework* and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with GDPR and relevant standards to protect Personal Data.

Reporting Data Breaches In certain instances, CIPD is required under GDPR to notify Personal Data Breaches to the ICO and the Data Subject. We have put in place procedures to deal with any suspected Personal Data Breach and our Director of Legal and Governance will log all Personal Data Breaches

on our data breach register and notify the ICO and Data Subjects where we are legally required to do so.

If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the person or team designated as the key point of contact for Personal Data Breaches in accordance with *CIPD's Data Breach Response Plan*. You should preserve all evidence relating to the potential Personal Data Breach.

(g) Transfer Limitation

GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by GDPR is not undermined. Data Transfers means transmitting, sending, viewing or accessing data in/to a different country from where it was originated.

To ensure compliance, CIPD must not transfer personal data to another country without appropriate safeguards in place. We have in place such safeguards to allow data transfers within the CIPD Group. For any other data transfers outside the EEA please contact the legal team.

(h) Data Subjects Rights & Requests

CIPD must allow Data Subjects to exercise certain rights in relation to their Personal Data. These include rights to:

- withdraw Consent to Processing at any time;
- receive certain information about the Data Controller's Processing activities;
- request access to their Personal Data that we hold;
- prevent our use of their Personal Data for direct marketing purposes;
- ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;
- restrict Processing in specific circumstances;
- challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;
- request a copy of an agreement under which Personal Data is transferred outside of the EEA;
- object to decisions based solely on Automated Processing, including profiling (ADM);
- prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;
- be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;
- make a complaint to the supervisory authority; and
- in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format.

If you receive a request from an individual in relation to any of the rights listed above, you must follow the steps set out in *GDPR FAQs & Privacy Principles* verifying the identity of the individual making the request where appropriate. Do not allow third parties to persuade you into disclosing Personal Data without proper authorisation.

4. Accountability

CIPD commits to providing adequate resources and having controls in place to ensure and to document GDPR compliance including:

(a) integrating data protection into internal documents including this policy, Related Policies, GDPR Guidelines and FAQs, Privacy Notices or Fair Processing Notices;

(b) regularly training CIPD People on GDPR, this Privacy Standard, Related Policies and GDPR Guidelines and FAQs and data protection matters including, for example, Data Subject's rights, Consent, legal basis, PIA and Personal Data Breaches. CIPD will maintain a record of training attendance by CIPD People;

(c) implementing Privacy by Design when Processing Personal Data and completing PIAs where Processing presents a high risk to rights and freedoms of Data Subjects; and

(d) regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

Training We are required to ensure all CIPD People have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance. You must complete all mandatory data privacy related training as indicated by the People team.

Privacy by Design & Data privacy Impact Assessment We are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

You must assess what Privacy by Design measures can be implemented on all programs/systems/processes that Process Personal Data by taking into account the following:

- the state of the art;
- the cost of implementation;
- the nature, scope, context and purposes of Processing; and
- the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.

We must also conduct PIAs in respect to high risk Processing. You should conduct a PIA (and discuss your findings with the legal team) when implementing major system or business change programs involving the Processing of Personal Data including:

- use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);
- Automated Processing including profiling and ADM;
- large scale Processing of Special Categories of Personal Data; and
- large scale, systematic monitoring of a publicly accessible area.

You must comply with *CIPD's guidelines on PIA*.

Automated Processing (including profiling) and Automated Decision Making Generally, ADM is prohibited when a decision has a legal or similar significant effect on an individual unless:

- a Data Subject has Explicitly Consented;
- the Processing is authorised by law; or
- the Processing is necessary for the performance of or entering into a contract.

If certain types of Special Categories of Personal Data are being Processed, then grounds (b) or (c) will not be allowed but such Special Categories of Personal Data can be Processed where it is necessary (unless less intrusive means can be used) for substantial public interest like fraud prevention.

If a decision is to be based solely on Automated Processing (including profiling), then Data Subjects must be informed when you first communicate with them of their right to object. This right must be explicitly brought to their attention and presented clearly and separately from other information. Further, suitable measures must be put in place to safeguard the Data Subject's rights and freedoms and legitimate interests.

We must also inform the Data Subject of the logic involved in the decision making or profiling, the significance and envisaged consequences and give the Data Subject the right to request human intervention, express their point of view or challenge the decision.

A PIA must be carried out before any Automated Processing (including profiling) or ADM activities are undertaken.

Direct Marketing We are subject to certain rules and privacy laws when marketing to our customers which means a Data Subject's prior consent is required for electronic direct marketing (i.e.by email, text or automated calls).

The limited exception for existing customers known as "soft opt in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information. A Data Subject's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be

suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

Sharing Personal Data Generally we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

You may only share the Personal Data we hold with another employee, agent or representative of the CIPD Group if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

You may only share the Personal Data we hold with third parties, such as our service providers and partners if:

(a) they have a need to know the information for the purposes of providing the contracted services;

(b) sharing the Personal Data complies with the Privacy Policy provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;

(c) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;

(d) the transfer complies with any applicable cross border transfer restrictions; and

(e) a fully executed written contract that contains GDPR approved third party clauses has been obtained.

Record Keeping GDPR requires us to keep full and accurate records of all our data Processing activities. You must keep and maintain accurate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents.

These records should include, at a minimum, the name and contact details of the Data Controller, clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place. In order to create such records, data maps should be created which should include the detail set out above together with appropriate data flows.

Audit You must regularly review all the systems and processes under your control to ensure they comply with this policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

Data Protection Officer (DPO) As part of our preparations for GDPR an internal cross-functional team (the GDPR Steering Committee) was set up with the remit to lead the CIPD's approach, roll out, provision of advice and monitoring of progress. They will continue to do so and as such will assume

the responsibilities of the ‘DPO’ including maintaining and implementing our policies and procedures relating to GDPR and ensuring we remain compliant. This work is overseen by our Director of Legal and Governance.

If you have any enquiry regarding GPDR and its application within the CIPD you can address them to the GDPR Steering Committee at dataprotection@cipd.co.uk

GLOSSARY

Automated Decision-Making (ADM): when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

Automated Processing: any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.

CIPD People: all employees, workers contractors, agency workers, consultants, associates and volunteers.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.

Data Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with GDPR. We are the Data Controller of all Personal Data relating to CIPD People and Personal Data used in our organisation for our own business purposes.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Privacy Impact Assessment (PIA): tools and assessments used to identify and reduce risks of a data processing activity. PIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the Processing of Personal Data.

EEA: the 28 countries in the EU, and Iceland, Liechtenstein and Norway.

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).

General Data Protection Regulation (GDPR): the General Data Protection Regulation (*(EU) 2016/679*). Personal Data is subject to the legal safeguards specified in GDPR.

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Special Categories of Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, membership number, financial data or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

GDPR Guidelines and FAQs: our guidelines provided to assist in interpreting and implementing this policy and Related Policies, available *here*.

Privacy Policy: separate notices setting out information that may be provided to Data Subjects when CIPD collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy) or they may be stand-alone, one time privacy statements covering Processing related to a specific purpose.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Related Policies: CIPD's policies, operating procedures or processes related to this policy and designed to protect Personal Data, available here: *Data Subject Rights; PIA Guidelines; Data Retention Policy; Information Security Framework; Data Breach Response Plan*

Special Categories of Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions.

END OF DOCUMENT