DIALIGHT DATA PROTECTION POLICY

1. INTERPRETATION

1.1 DEFINITIONS:

Affiliate(s): means in relation a party, any entity (corporate or otherwise) which at any time controls, is controlled by or which is under common control with such party, where "control" means the right to exercise, directly or indirectly, more than 50% of the voting securities of the party or relevant entity or the ability, directly or indirectly, to control or determine the management or general business decisions of such party or entity, whether by membership on the relevant board of directors or other governing body, by contract or by any other means

Group Personnel: all employees, workers, contractors, agency workers, consultants, directors, members and others.

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 the GDPR. We are the Data Controller of all Personal Data relating to our Group Personnel and Personal Data used in our business for our own commercial 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.

Data Protection Officer (DPO): the person required to be appointed in specific circumstances under the GDPR. Where a mandatory DPO has not been appointed, this term means a data protection manager or other voluntary appointment of a DPO or refers to the Group data privacy team with responsibility for data protection compliance.

EEA: the countries in the EU from time to time, and Iceland, Liechtenstein and Norway, and such other countries that may form part of the EEA from time to time.

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 the 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 Sensitive 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, location or date of birth) or an opinion about that person's actions or behaviour. Common examples include your personal address, DOB, personal email address, personal telephone number, gender, marital status, national insurance number (or national equivalent), bank account and salary details.

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.

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.

Sensitive 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.

2. INTRODUCTION

This data protection policy (the "**Policy**") sets out how Dialight plc and its Affiliates ("**we**", "**our**", "**us**", the "**Group**") handle the Personal Data of our customers, suppliers, employees, workers and other third parties.

Whilst the GDPR is EU legislation and is therefore focussed on safeguarding the Personal Data of EU Data Subjects, the GDPR (unlike previous EU data protection legislation) does have expanded territorial scope. This means that it will apply to and can be enforced against non-EU Data Controllers and Data Processors (such as Dialight Corporation) to the extent that they have access to the Personal Data relating to EU Data Subjects.

Therefore this Policy applies to all Group Personnel ("**you**", "**your**") and to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users or any other Data Subject.

You must read, understand and comply with this Policy when Processing Personal Data on our behalf and complete training on the GDPR requirements. You should already have completed the Dialight on-line training on data protection issued via the Thomson Reuters training portal or, if you are a new joiner, this will be sent through shortly. If you have not received this training, please contact the DPO or a member of the Dialight Legal Team at your earliest convenience.

This Policy sets out what we expect from you in order for the Group to comply with applicable law. Your compliance with this Policy is mandatory. Any breach of this Policy may result in disciplinary action.

This Policy is an internal document and cannot be shared with third parties, clients or regulators without prior authorisation from the DPO.

3. SCOPE

We recognise that the correct and lawful treatment of Personal Data will maintain confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. **The Group is exposed to potential fines of up to EUR20 million (approximately £18 million) or 4% of total worldwide annual turnover, whichever is higher and depending on the breach, for failure to comply with the provisions of the GDPR.**

All individual business areas, departments, line-mangers, supervisors and executive management are responsible for ensuring all Group Personnel comply with this Policy and need to implement appropriate practices, processes, controls and training to ensure such compliance.

The DPO is responsible for overseeing this Policy.

Please contact the DPO with any questions about the operation of this Policy or the GDPR or if you have any concerns that this Policy is not being or has not been followed. In particular, you must always contact the DPO in the following circumstances:

(a) If you are unsure of the lawful basis which you are relying on to process Personal Data (including the legitimate interests used by the Group) (see *Section 6.1* below);

(b) If you need to rely on Consent and/or need to capture Explicit Consent (see *Section 6.2* below);

(c) If you need to draft privacy notices (see *Section 6.3* below);

(d) If you are unsure about the retention period for the Personal Data being Processed (see *Section 10* below);

(e) If you are unsure about what security or other measures you need to implement to protect Personal Data (see *Section 11.1* below);

(f) If there has been a Personal Data Breach (*Section 11.2* below);

(g) If you are unsure on what basis to transfer Personal Data outside the EEA (see *Section 12* below);

(h) If you need any assistance dealing with any rights invoked by a Data Subject (see *Section 13*);

(i) Whenever you are engaging in a significant new, or change in, a Processing activity or plan to use Personal Data for purposes others than what it was collected for. In such circumstances you should work with the DPO to carry out and document a data privacy impact assessment ("**DPIA**") to assess the necessity, proportionality and risk associated with the Processing and agree on the appropriate risk mitigation and security measures required;

(j) If you plan to undertake any activities involving automated processing including profiling;

(k) If you need help complying with applicable law when carrying out direct marketing activities (see *Section 14.4* below); or

(l) If you need help with any contracts or other areas in relation to sharing Personal Data with third parties (including our vendors) (see *Section 14.5* below).

4. **HOW DOES DIALIGHT TYPICALLY USE YOUR PERSONAL DATA**

The Group will only process your Personal Data in accordance with the GDPR personal data protection principles (as summarised in Section 5 below). The Group primarily uses its employees' Personal Data to perform the contracts of employment with yourselves (or allow a third party to do this on our behalf) and to enable us to comply with legal obligations. The situations in which we will typically process Group employees' Personal Data are listed below:

- Making a decision about your recruitment or appointment.
- Determining the terms on which you work for us.
- Checking you are legally entitled to work for the Group.
- Paying you and, if you are an employee, deducting tax.
- Liaising with your pension provider.
- Administering the employment contract we have entered into with you.
- Business management and planning, including accounting and auditing.
- Conducting performance reviews, managing performance and determining performance requirements.
- Making decisions about salary reviews and compensation.
- Assessing qualifications for a particular job or task, including decisions about promotions.
- Gathering evidence for possible grievance or disciplinary hearings.
- Making decisions about your continued employment or engagement.
- Education, training and development requirements.
- Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work.
- Managing sickness absence.
- Complying with health and safety obligations.
- To prevent fraud.
- To monitor your use of our information and communication systems to ensure compliance with our IT policies.
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.

5. PERSONAL DATA PROTECTION PRINCIPLES

We adhere to the principles relating to Processing of Personal Data set out in the 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 allow Data Subjects 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).

6. LAWFULNESS, FAIRNESS, TRANSPARENCY

6.1 LAWFULNESS AND FAIRNESS

Personal data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The 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.

The GDPR allows Processing for specific purposes, some of which are set out below:

(a) the Data Subject has given his or her *Consent*;

(b) the Processing is *necessary* for the performance of a contract with the Data Subject;

(c) to meet our *legal compliance obligations*;

(d) to protect the Data Subject's *vital interests*;

(e) 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 need to be set out in applicable privacy notices (see *Section 5.3* below).

You must identify and record the legal ground being relied on for any Processing activity.

6.2 CONSENT

A Data Controller must only process Personal Data on the basis of one or more of the lawful bases set out in the GDPR and summarised in Section 6.1 (a)-(e) above, one of which includes 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 Processing Sensitive Personal Data and for cross border data transfers. Usually we will be relying on another legal basis (and not require Explicit Consent) to Process most types of Sensitive Data. Where Explicit Consent is required, you must issue a written communication or notice to the Data Subject to capture Explicit Consent.

You will need to evidence Consent captured and keep records of all Consents so that the Group can demonstrate compliance with Consent requirements.

6.3 TRANSPARENCY (NOTIFYING DATA SUBJECTS)

The 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. Such information must be provided through appropriate notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

Whenever we collect Personal Data directly from Data Subjects, including for human resources or employment purposes, we must provide the Data Subject with all the information required by the GDPR including the identity of the Data Controller and DPO, how and why we will use, Process, disclose, protect and retain that Personal Data through an appropriate written notice which must be presented when the Data Subject first provides the Personal Data.

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 the 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 the GDPR and on a basis which contemplates our proposed Processing of that Personal Data.

67 PURPOSE LIMITATION

Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes.

You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have Consented where necessary.

8. DATA MINIMISATION

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

You may only Process Personal Data when performing your job duties requires it. You cannot Process Personal Data for any reason unrelated to your job duties.

You may only collect Personal Data that you require for your job duties: 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.

9. ACCURACY

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

You will ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we 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.

10. STORAGE LIMITATION

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

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 or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

You will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require unless there is a legal requirement to hold the Personal Data for a longer time period. This includes requiring third parties to delete such data where applicable. Please contact the Group's DPO for case by case guidance if you have any queries in relation to data retention and destruction.

You will ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable privacy notice.

11. SECURITY INTEGRITY AND CONFIDENTIALITY

11.1 PROTECTING PERSONAL DATA

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

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 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 we hold. 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 Sensitive 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. Please seek guidance from the Dialight legal department before transferring Personal Data to a third party or entering into a contract which will give a third party access to Personal Data.

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

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

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

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

You must comply with and not attempt to circumvent the administrative, physical and technical IT safeguards in place from time to time. Please contact the Group IT Manager with any queries or for further information on our IT security protocol.

11.2 REPORTING A PERSONAL DATA BREACH

We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator 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 DPO or a member of the Dialight Legal Team. You should preserve all evidence relating to the potential Personal Data Breach.

12. TRANSFER LIMITATION

The GDPR restricts the transfer of Personal Data from countries within the EEA to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country. There does not have to be a physical transfer of Personal Data – if Personal Data relating to an EU Data Subject can be accessed electronically via the Group's network by an employee based outside the EEA, this amounts to a transfer of data outside the EEA.

You may only transfer Personal Data outside the EEA if one of the following conditions applies:

(a) the European Commission has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subjects' rights and freedoms;

(b) appropriate safeguards are in place such as binding corporate rules (BCR), standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism (a copy of which can be obtained from the DPO) or if the third party recipient is based in the USA, they are registered with the US Privacy Shield Program (please note that Dialight Corporation is not currently registered with the US Privacy Shield Program);

(c) the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or

(d) the transfer is necessary for one of the other reasons set out in the GDPR including the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interest.

You must ensure that one of the above conditions applies to any transfer of Personal Data from within the EEA to a country outside the EEA. Please contact the DPO or a member of the Dialight Legal Team for further guidance if you have any concerns or queries.

13. DATA SUBJECT'S RIGHTS AND REQUESTS

Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

(a) withdraw Consent to Processing at any time;

(b) receive certain information about the Data Controller's Processing activities;

(c) request access to their Personal Data that we hold;

(d) prevent our use of their Personal Data for direct marketing purposes;

(e) 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;

(f) restrict Processing in specific circumstances;

(g) challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;

(h) request a copy of an agreement under which Personal Data is transferred outside of the EEA;

(i) object to decisions based solely on any automated processing, including profiling;

(j) prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

(k) be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;

(l) make a complaint to the supervisory authority; and

(m) 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.

You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).

You must immediately forward any Data Subject request you receive to the DPO.

14. ACCOUNTABILITY

14.1 The Data Controller must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The Data Controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

The Group must have adequate resources and controls in place to ensure and to document GDPR compliance including:

(a) appointing a suitably qualified DPO (where necessary) and an executive accountable for data privacy. The Group Legal Counsel & Company Secretary is the executive responsible for GDPR matters for the Group (dsecretary@dialight.com);

(b) completing DPIAs in conjunction with the DPO where Processing presents a high risk to rights and freedoms of Data Subjects;

(c) regularly training Group Personnel on the GDPR. The Group will maintain a record of training attendance by Group Personnel; and

(d) conducting periodic reviews and audits to assess compliance.

14.2 RECORD KEEPING

The GDPR requires us to keep full and accurate records of all our data Processing activities. You must keep and maintain accurate corporate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents. Please work with the DPO to ensure that such records are maintained.

These records should include the name and contact details of the Data Controller and the DPO, 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.

14.3 TRAINING AND AUDIT

We are required to ensure all Group Personnel have undergone adequate training to enable them to comply with data privacy laws. Please support the DPO and the Legal Team by ensuring that you and, where applicable, your team complete the required training.

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.

14.4 DIRECT MARKETING

We are subject to certain rules and privacy laws when marketing to our customers.

For example, an EU Data Subject's prior Consent is required for electronic direct marketing (for example, 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.

You must comply with these guidelines and any other instruction from the DPO when direct marketing to customers **based in the EEA.**

14.5 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 our group (which includes our subsidiaries and our ultimate holding Group along with its subsidiaries) 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 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 notification 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.

You must consult with the DPO or the Dialight Legal Team before transferring any Personal Data to an external third party.

15. CHANGES TO THIS POLICY

We reserve the right to change this Policy at any time without notice to you so please check back regularly to obtain the latest copy of this Policy.

This Policy does not override any applicable national data privacy laws and regulations in countries where the Group operates.

END OF DOCUMENT