

## 1. Introduction

### 1.1 Background to the General Data Protection Regulation ('GDPR')

The General Data Protection Regulation 2016 replaces the EU Data Protection Directive of 1995 and supersedes the laws of individual Member States that were developed in compliance with the Data Protection Directive 95/46/EC. Its purpose is to protect the "rights and freedoms" of natural persons (i.e. living individuals) and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.

### 1.2 Definitions used by the organisation (drawn from the GDPR)

Material scope (Article 2) – the GDPR applies to the processing of personal data wholly or partly by automated means (i.e. by computer) and to the processing other than by automated means of personal data (i.e. paper records) that form part of a filing system or are intended to form part of a filing system.

Territorial scope (Article 3) – the GDPR will apply to all controllers that are established in the EU (European Union) who process the personal data of data subjects, in the context of that establishment. It will also apply to controllers outside of the EU that process personal data in order to offer goods and services, or monitor the behavior of data subjects who are resident in the EU.

### 1.3 Article 4 definitions

Establishment – the main establishment of the controller in the EU will be the place in which the controller makes the main decisions as to the purpose and means of its data processing activities. The main establishment of a processor in the EU will be its administrative centre. If a controller is based outside the EU, it will have to appoint a representative in the jurisdiction in which the controller operates to act on behalf of the controller and deal with supervisory authorities.

Personal data – 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.

Special categories of personal data – personal data 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.

Data controller – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are

*Classification\_3*

# DATA PROTECTION POLICY STATEMENT (TIER 1)

## Document Control

Reference: GDPR DOC 1.0

Issue No: 1

Issue Date: 16<sup>th</sup> March 2018

Page: 2 of 14

determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Data subject – any living individual who is the subject of personal data held by an organisation.

Processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Profiling – is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behavior. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

Personal data breach – a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

Data subject consent - means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

Child – the GDPR defines a child as anyone under the age of 16 years old, although this may be lowered to 13 by Member State law. The processing of personal data of a child is only lawful if parental or custodian consent has been obtained. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child.

Third party – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Filing system – any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

*Classification\_3*

# DATA PROTECTION POLICY STATEMENT (TIER 1)

## Document Control

Reference: GDPR DOC 1.0

Issue No: 1

Issue Date: 16<sup>th</sup> March 2018

Page: 3 of 14

## 2. Policy statement

- 2.1 The Directors of Optichrome Limited located at 98-100 Maybury Road, Woking, GU21 5HX are committed to compliance with all relevant EU and Member State laws in respect of personal data, and the protection of the "rights and freedoms" of individuals whose information Optichrome Limited collects and processes in accordance with the General Data Protection Regulation (GDPR).
- 2.2 Compliance with the GDPR is described by this policy and other relevant policies along with connected processes and procedures.
- 2.3 The GDPR and this policy apply to all of Optichrome Limited's personal data processing functions, including those performed on customers', clients', employees', suppliers' and partners' personal data, and any other personal data the organisation processes from any source.
- 2.4 Optichrome Limited has established objectives for data protection and privacy, which are in our GDPR Objectives Record.
- 2.5 The Technical Director as GDPR Owner is responsible for reviewing the register of processing annually in the light of any changes to Optichrome Limited's activities (as determined by changes to the data inventory register and the management review) and to any additional requirements identified by means of data protection impact assessments. These records will be available on the supervisory authority's request.
- 2.6 This policy applies to all Employees/Staff and Interested Parties of Optichrome Limited such as outsourced suppliers. Any breach of the GDPR will be dealt with under Optichrome Limited's disciplinary policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.
- 2.7 Partners and any third parties working with or for Optichrome Limited, and who have or may have access to personal data, will be expected to have read, understood and to comply with this policy. No third party may have access to personal data held by Optichrome Limited without having first entered into a data confidentiality agreement or contract, which imposes on the third party obligations no less onerous than those to which Optichrome Limited is committed, and which gives Optichrome Limited the right to audit compliance with the agreement.

Optichrome Limited's objectives for compliance with the GDPR:

- are consistent with this policy
- are measurable
- take into account GDPR and ISO 27001:2013 requirements and the results from risk assessments and risk treatments.
- are monitored
- are communicated

In order to achieve these objectives, Optichrome Limited has determined:

- what will be done
- what resources will be required
- who will be responsible
- when it will be completed
- how the results will be evaluated

*Classification\_3*

# DATA PROTECTION POLICY STATEMENT (TIER 1)

## Document Control

Reference: GDPR DOC 1.0

Issue No: 1

Issue Date: 16<sup>th</sup> March 2018

Page: 4 of 14

### 3. Responsibilities and roles under the General Data Protection Regulation

- 3.1 Optichrome Limited is both data controller and/or data processor under the GDPR.
- 3.2 Top Management and all those in managerial or supervisory roles throughout Optichrome Limited are responsible for developing and encouraging good information handling practices within Optichrome Limited; responsibilities are set out in individual job descriptions.
- 3.3 The Technical Director as GDPR Owner is a member of the senior management team and is accountable for the management of personal data within Optichrome Limited and for ensuring that compliance with data protection legislation and good practice can be demonstrated. This accountability includes:
  - 3.3.1 development and implementation of the GDPR as required by this policy; and
  - 3.3.2 security and risk management in relation to compliance with the policy.
- 3.4 The Technical Director as GDPR Owner has specific responsibilities in respect of procedures such as the Subject Access Request Procedure and is the first point of call for Employees/Staff seeking clarification on any aspect of data protection compliance.
- 3.5 Compliance with data protection legislation is the responsibility of all Employees/Staff of Optichrome Limited who process personal data.
- 3.6 Optichrome Limited's Training Policy sets out specific training and awareness requirements in relation to specific roles and Employees/Staff of Optichrome Limited generally.
- 3.7 Employees/Staff of Optichrome Limited are responsible for ensuring that any personal data about them and supplied by them to Optichrome Limited is accurate and up-to-date.

### 4. Data protection principles

All processing of personal data must be conducted in accordance with the data protection principles as set out in Article 5 of the GDPR. Optichrome Limited's policies and procedures are designed to ensure compliance with the principles.

- 4.1 Personal data must be processed lawfully, fairly and transparently  
Lawful – identify a lawful basis before you can process personal data. These are often referred to as the "conditions for processing", for example consent.

Fairly in order for processing to be fair, the data controller has to make certain information available to the data subjects as practicable. This applies whether the personal data was obtained directly from the data subjects or from other sources.

The GDPR has increased requirements about what information should be available to data subjects, which is covered in the 'Transparency' requirement.

*Classification\_3*

# DATA PROTECTION POLICY STATEMENT (TIER 1)

## Document Control

Reference: GDPR DOC 1.0

Issue No: 1

Issue Date: 16<sup>th</sup> March 2018

Page: 5 of 14

Transparently – the GDPR includes rules on giving privacy information to data subjects in Articles 12, 13 and 14. These are detailed and specific, placing an emphasis on making privacy notices understandable and accessible. Information must be communicated to the data subject in an intelligible form using clear and plain language.

Optichrome Limited's Privacy Notice Procedure is set out in GDPR DOC 2.1 and the Privacy Notice is recorded in GDPR REC 4.1.

The specific information that must be provided to the data subject must, as a minimum, include:

- 4.1.1 the identity and the contact details of the controller and, if any, of the controller's representative;
  - 4.1.2 the contact details of the GDPR Owner;
  - 4.1.3 the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
  - 4.1.4 the period for which the personal data will be stored;
  - 4.1.5 the existence of the rights to request access, rectification, erasure or to object to the processing, and the conditions (or lack of) relating to exercising these rights, such as whether the lawfulness of previous processing will be affected;
  - 4.1.6 the categories of personal data concerned;
  - 4.1.7 the recipients or categories of recipients of the personal data, where applicable;
  - 4.1.8 where applicable, that the controller intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data;
  - 4.1.9 any further information necessary to guarantee fair processing.
- 4.2 Personal data can only be collected for specific, explicit and legitimate purposes  
Data obtained for specified purposes must not be used for a purpose that differs from those formally notified to the supervisory authority as part of Optichrome Limited's GDPR register of processing. Privacy Procedure GDPR DOC 2.1 sets out the relevant procedures.
- 4.3 Personal data must be adequate, relevant and limited to what is necessary for processing
- 4.3.1 The GDPR Owner is responsible for ensuring that Optichrome Limited does not collect information that is not strictly necessary for the purpose for which it is obtained (refer to DPIA Tool GDPR REC 4.4 for the data flow/mapping).
  - 4.3.2 All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must include a fair processing statement or link to privacy statement and approved by the GDPR Owner.
  - 4.3.3 The GDPR Owner will ensure that, on an annual basis all data collection methods are reviewed to ensure that collected data continues to be adequate, relevant and not excessive (Data Protection Impact Assessment Procedure GDPR DOC 2.4 and DPIA Tool GDPR REC 4.4).

*Classification\_3*

# DATA PROTECTION POLICY STATEMENT (TIER 1)

## Document Control

Reference: GDPR DOC 1.0

Issue No: 1

Issue Date: 16<sup>th</sup> March 2018

Page: 6 of 14

- 4.4 Personal data must be accurate and kept up to date with every effort to erase or rectify without delay
- 4.4.1 Data that is stored by the data controller must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.
- 4.4.2 The GDPR Owner is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.
- 4.4.3 It is also the responsibility of the data subject to ensure that data held by Optichrome Limited is accurate and up to date. Completion of any application form by a data subject will include a statement that the data contained therein is accurate at the date of submission. Employees are required to notify Optichrome Limited of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of Optichrome Limited to ensure that any notification regarding change of circumstances is recorded and acted upon.
- 4.4.4 The GDPR Owner is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.
- 4.4.5 On at least an annual basis, the GDPR Owner will review the retention dates of all the personal data processed by Optichrome Limited, by reference to the data inventory, and will identify any data that is no longer required in the context of the registered purpose. This data will be securely deleted/destroyed in line with the Secure Disposal of Storage Media Procedure GDPR-C DOC 11.2.7.
- 4.4.6 The GDPR Owner is responsible for responding to requests for rectification from data subjects within one month (Subject Access Request Procedure GDPR DOC 2.2). This can be extended to a further two months for complex requests. If Optichrome Limited decides not to comply with the request, the GDPR Owner must respond to the data subject to explain its reasoning and inform them of their right to complain to the supervisory authority and seek judicial remedy.
- 4.4.7 The GDPR Owner is responsible for making appropriate arrangements that, where third-party organisations may have been passed inaccurate or out-of-date personal data, to inform them that the information is inaccurate and/or out of date and is not to be used to inform decisions about the individuals concerned; and for passing any correction to the personal data to the third party where this is required.
- 4.5 Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.
- 4.5.1 Where personal data is retained beyond the processing date, it will be encrypted in order to protect the identity of the data subject in the event of a data breach.
- 4.5.2 Personal data will be retained in line with the Retention of Records Procedure (GDPR DOC 2.3) and, once its retention date is passed, it must be securely destroyed as set out in this procedure.
- 4.5.3 The GDPR Owner must specifically approve any data retention that exceeds the retention periods defined in Retention of Records Procedure (GDPR DOC

*Classification\_3*

# DATA PROTECTION POLICY STATEMENT (TIER 1)

## Document Control

Reference: GDPR DOC 1.0

Issue No: 1

Issue Date: 16<sup>th</sup> March 2018

Page: 7 of 14

2.3), and must ensure that the justification is clearly identified and in line with the requirements of the data protection legislation. This approval must be written.

- 4.6 Personal data must be processed in a manner that ensures the appropriate security  
The GDPR Owner will carry out a risk assessment taking into account all the circumstances of Optichrome Limited's controlling or processing operations.

In determining appropriateness, the GDPR Owner should also consider the extent of possible damage or loss that might be caused to individuals (e.g. staff or customers) if a security breach occurs, the effect of any security breach on Optichrome Limited itself, and any likely reputational damage including the possible loss of customer trust.

When assessing appropriate technical measures, the GDPR Owner will consider the following:

- Password protection;
- Automatic locking of idle terminals;
- Removal of access rights for USB and other memory media;
- Virus checking software and firewalls
- Role-based access rights including those assigned to temporary staff;
- Encryption of devices that leave the organisations premises such as laptops;
- Security of local and wide area networks;
- Privacy enhancing technologies such as pseudonymisation and anonymisation;
- Identifying appropriate international security standards relevant to Optichrome Limited.

When assessing appropriate organisational measures the GDPR Owner will consider the following:

- The appropriate training levels throughout Optichrome Limited;
- Measures that consider the reliability of employees (such as references etc.);
- The inclusion of data protection in employment contracts;
- Identification of disciplinary action measures for data breaches;
- Monitoring of staff for compliance with relevant security standards;
- Physical access controls to electronic and paper based records;
- Adoption of a clear desk policy;
- Storing of paper based data in lockable fire-proof cabinets;
- Restricting the use of portable electronic devices outside of the workplace;
- Restricting the use of employee's own personal devices bbeing used in the workplace;
- Adopting clear rules about passwords;
- Making regular backups of personal data and storing the media off-site;
- The imposition of contractual obligations on the importing organisations to take appropriate security measures when transferring data outside the EEA.

These controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed.

*Classification\_3*



# DATA PROTECTION POLICY STATEMENT (TIER 1)

## Document Control

Reference: GDPR DOC 1.0

Issue No: 1

Issue Date: 16<sup>th</sup> March 2018

Page: 8 of 14

Optichrome Limited's compliance with this principle is contained in its Information Security Management System (ISMS), which has been developed in line with ISO 27001:2013 and the information security policies.

#### 4.7 The controller must be able to demonstrate compliance with the GDPR's other principles (accountability)

The GDPR includes provisions that promote accountability and governance. These complement the GDPR's transparency requirements. The accountability principle in Article 5(2) requires Optichrome Limited to demonstrate that you comply with the principles and states explicitly that this is your responsibility.

Optichrome Limited will demonstrate compliance with the data protection principles by implementing data protection policies, adhering to codes of conduct, implementing technical and organisational measures, as well as adopting techniques such as data protection by design, DPIAs, breach notification procedures and incident response plans.

## 5. Data subjects' rights

### 5.1 Data subjects have the following rights regarding data processing, and the data that is recorded about them:

- 5.1.1 To make subject access requests regarding the nature of information held and to whom it has been disclosed.
- 5.1.2 To prevent processing likely to cause damage or distress.
- 5.1.3 To prevent processing for purposes of direct marketing.
- 5.1.4 To be informed about the mechanics of automated decision-taking process that will significantly affect them.
- 5.1.5 To not have significant decisions that will affect them taken solely by automated process.
- 5.1.6 To sue for compensation if they suffer damage by any contravention of the GDPR.
- 5.1.7 To take action to rectify, block, erased, including the right to be forgotten, or destroy inaccurate data.
- 5.1.8 To request the supervisory authority to assess whether any provision of the GDPR has been contravened.
- 5.1.9 To have personal data provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller.
- 5.1.10 To object to any automated profiling that is occurring without consent.

### 5.2 Optichrome Limited ensures that data subjects may exercise these rights:

- 5.2.1 Data subjects may make data access requests as described in Subject Access Request Procedure (GDPR DOC 2.2); this procedure also describes how Optichrome Limited will ensure that its response to the data access request complies with the requirements of the GDPR.

*Classification\_3*



# DATA PROTECTION POLICY STATEMENT (TIER 1)

## Document Control

Reference: GDPR DOC 1.0

Issue No: 1

Issue Date: 16<sup>th</sup> March 2018

Page: 9 of 14

5.2.2 Data subjects have the right to complain to Optichrome Limited related to the processing of their personal data, the handling of a request from a data subject and appeals from a data subject on how complaints have been handled in line with the Complaints Procedure (GDPR DOC 2.9).

## 6. Consent

- 6.1 Optichrome Limited understands 'consent' to mean that it has been explicitly and freely given, and a specific, informed and unambiguous indication of the data subject's wishes that, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The data subject can withdraw their consent at any time.
- 6.2 Optichrome Limited understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing.
- 6.3 There must be some active communication between the parties to demonstrate active consent. Consent cannot be inferred from non-response to a communication.
- 6.4 For sensitive data, explicit written consent (Consent Procedure GDPR DOC 2.7) of data subjects must be obtained unless an alternative legitimate basis for processing exists.
- 6.5 In most instances, consent to process personal and sensitive data is obtained routinely by Optichrome Limited using standard consent documents Contracts of Employment or Client Contracts and Agreements e.g. when a new client signs a contract, or during induction for participants on programmes.
- 6.6 Where Optichrome Limited provides online services to children, parental or custodial authorisation must be obtained. This requirement applies to children under the age of 16 (unless the Member State has made provision for a lower age limit, which may be no lower than 13). Not currently part of our operations.

## 7. Security of data

- 7.1 All Employees/Staff are responsible for ensuring that any personal data that Optichrome Limited holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by Optichrome Limited to receive that information and has entered into a confidentiality agreement.
- 7.2 All personal data should be accessible only to those who need to use it, and access may only be granted in line with the Access Control Policy. All personal data should be treated with the highest security and must be kept:
  - in a lockable room with controlled access; and/or
  - in a locked drawer or filing cabinet; and/or
  - if computerised, password protected in line with corporate requirements in the Access Control Policy and/or
  - stored on (removable) computer media which are encrypted.

*Classification\_3*

# DATA PROTECTION POLICY STATEMENT (TIER 1)

## Document Control

Reference: GDPR DOC 1.0

Issue No: 1

Issue Date: 16<sup>th</sup> March 2018

Page: 10 of 14

- 7.3 Care must be taken to ensure that PC screens and terminals are not visible except to authorised Employees/Staff of Optichrome Limited. All Employees/Staff are required to sign our Employee Security User Guide before they are given access to organisational information of any sort, which details rules on screen time-outs.
- 7.4 Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit authorisation. As soon as manual records are no longer required for day-to-day client support, they must be locked away.
- 7.5 Personal data may only be deleted or disposed of in line with the Retention of Records Procedure (GDPR DOC 2.3). Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed and immediately destroyed before disposal.
- 7.6 Processing of personal data 'off-site' presents a potentially greater risk of loss, theft or damage to personal data. Staff must be specifically authorised to process data off-site.

## 8. Disclosure of data

- 8.1 Optichrome Limited must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All Employees/Staff should exercise caution when asked to disclose personal data held on another individual to a third party. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of Optichrome Limited's business.
- 8.2 All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the GDPR Owner.

## 9. Retention and disposal of data

- 9.1 Optichrome Limited shall not keep personal data in a form that permits identification of data subjects for longer a period than is necessary, in relation to the purpose(s) for which the data was originally collected.
- 9.2 Optichrome Limited may store data for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.
- 9.3 The retention period for each category of personal data will be set out in the Retention of Records Procedure (GDPR DOC 2.3) along with the criteria used to determine this period including any statutory obligations Optichrome Limited has to retain the data.
- 9.4 Optichrome Limited's data retention and data disposal procedures will apply in all cases.

*Classification\_3*

# DATA PROTECTION POLICY STATEMENT (TIER 1)

## Document Control

Reference: GDPR DOC 1.0

Issue No: 1

Issue Date: 16<sup>th</sup> March 2018

Page: 11 of 14

- 9.5 Personal data must be disposed of securely in accordance with the sixth principle of the GDPR – processed in an appropriate manner to maintain security, thereby protecting the “rights and freedoms” of data subjects. Any disposal of data will be done in a secure manner.

## 10. Data transfers

- 10.1 All exports of data from within the European Economic Area (EEA) to non-European Economic Area countries (referred to in the GDPR as ‘third countries’) are unlawful unless there is an appropriate “level of protection for the fundamental rights of the data subjects.

The transfer of personal data outside of the EEA is prohibited unless one or more of the specified safeguards, or exceptions, apply:

### 10.1.1 An adequacy decision

The European Commission can and does assess third countries, a territory and/or specific sectors within third countries to assess whether there is an appropriate level of protection for the rights and freedoms of natural persons. In these instances no authorisation is required.

Countries that are members of the European Economic Area (EEA) but not of the EU are accepted as having met the conditions for an adequacy decision.

A list of countries that currently satisfy the adequacy requirements of the Commission are published in the *Official Journal of the European Union*.

[http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index\\_en.htm](http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm)

### 10.1.2 Privacy Shield

If Optichrome Limited wishes to transfer personal data from the EU to an organisation in the United States it should check that the organisation is signed up with the Privacy Shield framework at the U.S. Department of Commerce. The obligation applying to companies under the Privacy Shield are contained in the “Privacy Principles”. The US DOC is responsible for managing and administering the Privacy Shield and ensuring that companies live up to their commitments. In order to be able to certify, companies must have a privacy policy in line with the Privacy Principles e.g. use, store and further transfer the personal data according to a strong set of data protection rules and safeguards. The protection given to the personal data applies regardless of whether the personal data is related to an EU resident or not. Organisations must renew their “membership” to the Privacy Shield on an annual basis. If they do not, they can no longer receive and use personal data from the EU under that framework.

#### Assessment of adequacy by the data controller

In making an assessment of adequacy, the UK based exporting controller should take account of the following factors:

- the nature of the information being transferred;
- the country or territory of the origin, and final destination, of the information;
- how the information will be used and for how long;

*Classification\_3*

# DATA PROTECTION POLICY STATEMENT (TIER 1)

## Document Control

Reference: GDPR DOC 1.0

Issue No: 1

Issue Date: 16<sup>th</sup> March 2018

Page: 12 of 14

- the laws and practices of the country of the transferee, including relevant codes of practice and international obligations; and the security measures that are to be taken as regards the data in the overseas location.

### 10.1.3 Binding Corporate Rules

Optichrome Limited may adopt approved binding corporate rules for the transfer of data outside the EU. This requires submission to the relevant supervisory authority for approval of the rules that Optichrome Limited is seeking to rely upon.

### 10.1.4 Model contract clauses

Optichrome Limited may adopt approved model contract clauses for the transfer of data outside of the EEA. If Optichrome Limited adopts the model contract clauses approved by the relevant supervisory authority there is an automatic recognition of adequacy.

### 10.1.5 Exceptions

In the absence of an adequacy decision, Privacy Shield membership, binding corporate rules and/or model contract clauses, a transfer of personal data to a third country or international organisation shall only take place on one of the following conditions:

- the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims; and/or
- the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.

## 11. Information asset register/data inventory

11.1 Optichrome Limited has established a data inventory and data flow process as part of its approach to address risks and opportunities throughout its GDPR compliance project. Optichrome Limited's data inventory and data flow determines (GDPR DOC 2.4, and GDPR REC 4.4):

- business processes that use personal data;
- source of personal data;
- volume of data subjects;

*Classification\_3*

# DATA PROTECTION POLICY STATEMENT (TIER 1)

## Document Control

Reference: GDPR DOC 1.0

Issue No: 1

Issue Date: 16<sup>th</sup> March 2018

Page: 13 of 14

- description of each item of personal data;
- processing activity;
- maintains the inventory of data categories of personal data processed;
- documents the purpose(s) for which each category of personal data is used;
- recipients, and potential recipients, of the personal data;
- the role of the Optichrome Limited throughout the data flow;
- key systems and repositories;
- any data transfer and
- all retention and disposal requirements.

11.2 Optichrome Limited is aware of any risks associated with the processing of particular types of personal data.

11.2.1 Optichrome Limited assesses the level of risk to individuals associated with the processing of their personal data. Data protection impact assessments (DPIAs) (DPIA Procedure GDPR DOC 2.4 and GDPR REC 4.4) are carried out in relation to the processing of personal data by Optichrome Limited, and in relation to processing undertaken by other organisations on behalf of Optichrome Limited.

11.2.2 Optichrome Limited shall manage any risks identified by the risk assessment in order to reduce the likelihood of a non-conformance with this policy.

11.2.3 Where a type of processing, in particular using new technologies and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons, Optichrome Limited shall, prior to the processing, carry out a DPIA of the impact of the envisaged processing operations on the protection of personal data. A single DPIA may address a set of similar processing operations that present similar high risks.

11.2.4 Where, as a result of a DPIA it is clear that Optichrome Limited is about to commence processing of personal data that could cause damage and/or distress to the data subjects, the decision as to whether or not Optichrome Limited may proceed must be escalated for review to the GDPR Owner.

11.2.5 The GDPR Owner shall, if there are significant concern, either as to the potential damage or distress, or the quantity of data concerned, escalate the matter to the supervisory authority.

11.2.6 Appropriate controls have been implemented as per our existing ISO 27001:2013 ISMS and applied to reduce the level of risk associated with processing individual data to an acceptable level, by reference to Optichrome Limited's documented risk acceptance criteria and the requirements of the GDPR.

### ***Document Owner and Approval***

The GDPR Owner is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the review requirements stated above.

A current version of this document is available to all members of staff.

*Classification\_3*

# DATA PROTECTION POLICY STATEMENT (TIER 1)

## Document Control

Reference: GDPR DOC 1.0  
Issue No: 1  
Issue Date: 16<sup>th</sup> March 2018  
Page: 14 of 14

This policy was approved by the Directors on 16<sup>th</sup> March 2018 and is issued on a version controlled basis under the signature of the Managing Director.

Signature:



Date: 16<sup>th</sup> March 2018

## Change History Record

Issue	Description of Change	Approval	Date of Issue
1	Initial issue	M Burford	16 <sup>th</sup> March 2018

*Classification\_3*