PRIVACY NOTICE

HODGE

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.

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

The GDPR will apply to all data 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 data controllers outside of the EU that process personal data in order to offer goods and services, or monitor the behaviour of data subjects who are resident in the EU.

2. Notice statement

2.1 Hodge, located at One Central Square, Cardiff, CF10 1FS is 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 (data subject) whose information Hodge collects and processes in accordance with the General Data Protection Regulation (GDPR).

2.2 Hodge and Hodge Bank are trading names of Julian Hodge Bank Limited which is registered in England and Wales (No. 743437). Hodge Lifetime is a trading name of Julian Hodge Bank Limited and Hodge Life Assurance Company Limited which is registered in England and Wales (No. 837457).

2.3 Hodge's compliance with the GDPR is described by this Notice statement.

2.4 The GDPR and this Notice applies to all Hodge'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.

2.5 Hodge has established objectives for data protection and privacy of personal data.

2.6 The Data Protection Officer (DPO) is responsible for reviewing the register of processing annually in light of any changes to the Hodge'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. This register will be available on the supervisory authority's request.

2.7 Partners and any third parties working with or for Hodge and who have or may have access to customer personal data, are obliged to have read, understood and to comply with this Notice. No third party may have access to customer personal data held by Hodge without having first entered into a data confidentiality agreement which imposes on the third-party obligations no less onerous than those to which Hodge is committed, and which gives Hodge the right to audit compliance with the agreement.

3. Data protection principles

All processing of personal data is conducted in accordance with the data protection principles as set out in Article 5 of the GDPR. Hodge's policies and procedures have been designed to ensure compliance with those principles.

3.1 **Personal data must be processed lawfully, fairly and transparently.**

The personal details provided to Hodge are subject to the provisions of the GDPR.

The information will be retained only for as long as necessary in accordance with Hodge's Retention Policy and may be stored on paper or in electronic format.

The personal details held may be used for the following purposes:

- Administering an application;
- Verifying identity and anti-money laundering checks;
- Assisting in fraud prevention;
- Reporting to regulators and authorities;
- Product analysis.

The information held may be shared with the following parties:

- Hodge's approved service providers in relation to the processing of an application;
- Other members of the group to which Hodge belongs, including its subsidiaries and associated companies;
- Regulators or authorities where required or permitted by law.

The data subject has the right to request access to their personal information held by Hodge. To do so, this request must be made in writing using our Data Subject Access Request Process. Under certain circumstances the request can also be undertaken via phone call.

3. Data protection principles (continued)

3.2 **Personal data must be adequate, relevant and limited to what is necessary for processing.**

3.2.1 Hodge's DPO is responsible for ensuring that Hodge does not collect information that is not strictly necessary for the purpose for which it is obtained.

3.2.2 All data collection forms (electronic or paper-based), including data collection requirements in new information systems, includes a fair processing statement or link to a privacy statement and be approved by the DPO.

3.2.3 The DPO will ensure that, on an annual basis all data collection methods are reviewed by Hodge's Internal Audit / Assurance function to ensure that collected data continues to be adequate, relevant and not excessive.

3.3 **Personal data must be accurate and kept up to date with every effort to erase or rectify without delay.**

3.3.1 Data that is stored by Hodge has been reviewed and updated as necessary.

3.3.2 Processes are in place to ensure that when data is collected it is accurate.

3.3.3 All staff are trained in the importance of collecting accurate data and maintaining it.

3.3.4 It is the responsibility of the data subject to ensure that data held by Hodge is accurate and up to date. Completion of a registration or application form by a data subject will include a statement that the data contained therein is accurate at the date of submission.

3.3.5 The data subject is required to notify Hodge of any changes of circumstance to ensure personal records to be updated accordingly. Hodge will ensure that any notification regarding change of circumstances is recorded and acted upon as necessary.

3.3.6 All processes and policies are updated to ensure personal data capture is accurate and up to date. The DPO 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.

3. Data protection principles (continued)

3.3.7 On at least an annual basis, the DPO will review the retention dates of all the personal data processed by Hodge 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.

3.3.8 The DPO will ensure that requests for rectification from data subjects are addressed within one month (Data Subject Access Request Process). This can be extended for a further month for complex requests. If Hodge decides not to comply with the request, the DPO will respond to the data subject to explain its reasoning and inform them of their right to complain to the supervisory authority (Information Commissioner's Office - ICO) and seek judicial remedy.

3.3.9 The DPO is responsible for making appropriate arrangements that, where third-party organisations may have been passed inaccurate or out-of-date personal data, they are informed 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.

3.4 **Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.**

3.4.1 Where personal data is retained beyond Hodge's retention policy, it will be minimized, held in an encrypted format and where possible pseudonymised in order to protect the identity of the data subject in the event of a data breach.

3.4.2 Personal data will be retained in line with Hodge's Retention Policy and, once its retention date is passed, it will be securely destroyed as set out in this Notice and the relevant departmental procedure.

3.4.3 The DPO will specifically approve any data retention that exceeds the retention periods defined in Hodge's Retention Policy and will ensure that the justification is clearly identified and in line with the requirements of the data protection legislation. This approval will be kept in written form and on record for future reference.

3. Data protection principles (continued)

3.5 **Personal data must be processed in a manner that ensures appropriate security.**

Hodge undertakes regular risk assessments, taking into account all of the circumstances of Hodge's controlling or processing operations. This assessment takes into account the extent of possible damage or loss that might be caused to the data subject (e.g. staff or customers) if a security breach occurs, the effect of any security breach on Hodge itself, and any likely reputational damage including the possible loss of customer trust has been considered.

The following technical measures are in place to ensure security of data:

- Password protection
- Automatic locking of idle terminals;
- Removal of access rights for USB and other memory;
- 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 anonymization;
- Identifying appropriate international security standards relevant to Hodge.

3. Data protection principles (continued)

3.5 The following operational measures are in place:

- Appropriate training levels throughout Hodge;
- 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 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 data subjects whose data is being processed.

3.6 **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 Hodge to demonstrate that it complies with the principles and states explicitly what Hodge's responsibility is.

Hodge has implemented data protection policies, codes of conduct, relevant technical and organisational measures, as well as adopting techniques such as data protection by design, Data Protection Impact Assessments, breach notification procedures and incident response plans.

4. Data subjects' rights

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

4.1.1 To make subject access requests regarding the nature of information held and to whom it has been disclosed.

4.1.2 To prevent processing likely to cause damage or distress.

4.1.3 To prevent processing for purposes of direct marketing.

4.1.4 To be informed about the mechanics of any automated decision-taking process that will significantly affect them.

4.1.5 To not have significant decisions that will affect them made solely by automated process.

4.1.6 To sue for compensation if they suffer damage by any breach of the GDPR.

4.1.7 To take action to rectify, block, erase, including the right to be forgotten, or destroy inaccurate data.

4.1.8 To request the supervisory authority to assess whether any provision of the GDPR has been breached.

4.1.9 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.

4.1.10 To object to any automated profiling that is occurring without consent.

4.2 Hodge ensures that data subjects can exercise these rights:

4.2.1 Data subjects can make data access requests as described in the Data Subject Access Request Procedure. This procedure describes how Hodge ensures that its response to the request complies with the requirements of the GDPR.

4.2.2 Data subjects have the right to complain to Hodge in relation 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.

4.2.3 Data subjects also have the right to complain to the ICO if they are not satisfied with how their Data Subject Access Request (DSAR) is handled.

4.2.4 Hodge has detailed the process and procedures within its SAR Procedure and Complaints procedure.

5. Consent

5.1 Hodge understands 'consent' to mean that it has been explicitly and freely given, and represents a specific, informed and unambiguous indication of the data subject's wishes that, by statement or by a clear affirmative action, signifies their agreement to the processing of personal data relating to them.

5.2 The data subject can withdraw their consent at any time.

5.3 Hodge 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.

5.4 Hodge accepts that consent obtained under duress or on the basis of misleading information is not a valid basis for processing.

5.5 Hodge ensure there is active communication with the data subject (s) to demonstrate active consent. Hodge ensures consent is not inferred from non-response to a communication.

5.6 For sensitive data, such as race, political views, sexual orientation or health issues, Hodge ensure s explicit written consent is obtained from the data subjects unless there a legitimate basis for processing exists.

5.7 In most instances, consent to process personal and sensitive data is obtained routinely by Hodge using standard consent documents e.g. when a new client signs a contract, applies via an application.

5.8 Where Hodge provides online services to children it ensures parental and/or custodial authorisation is obtained. This requirement applies to children under the age of 16.

6. Security of data

6.1 All personal data that Hodge holds and for which it is responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by Hodge to receive that information and has entered into a confidentiality agreement.

7. Disclosure of data

7.1 Hodge ensures that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. Hodge exercises caution when asked to disclose personal data held on another individual to a third party and only does so when disclosure of the information is relevant to, and necessary for, the conduct of Hodge's business.

7.2 All requests to provide data for one of these reasons is supported by appropriate paperwork and all such disclosures are specifically authorised by the DPO.

8. Retention and disposal of data

8.1 Hodge does 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.

8.2 Where Hodge stores and/or processes personal data for longer periods it does so solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. Storage is subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.

8.3 The retention period for each category of personal data is set out in Hodge's Retention Policy along with the criteria used to determine this period including any statutory obligations Hodge has to retain the data.

8.4 Hodge's data retention and data disposal procedures apply in all cases.

8.5 Personal data is disposed of securely in accordance with the fifth principle of the GDPR – processed in an appropriate manner to maintain security, thereby protecting the "rights and freedoms" of data subjects.

HODGE

Send requests to the DPO in writing to this address:
Data Protection Officer,
Hodge , One Central Square,
Cardiff, CF10 1FS.

Registered number 0390216